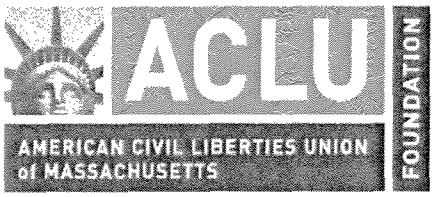

Laura Rótolo
Staff Counsel
ACLU of Massachusetts
211 Congress Street
Boston, MA 02110
lrotolo@aclum.org
(617) 482-3170 x311

December 9, 2013

Carmen M. Ortiz
United States Attorney for the District of Massachusetts
John Joseph Moakley
United States Federal Courthouse
1 Courthouse Way, Suite 9200
Boston, MA 02210

Dear U.S. Attorney Ortiz:

This letter is a request under the Freedom of Information Act, 5 U.S.C. § 552 submitted on behalf of the American Civil Liberties Union Foundation of Massachusetts (ACLUM). We are seeking public records regarding the Joint Terrorism Task Force that operates in Massachusetts (Massachusetts JTTF). For the reasons stated below, we also request expedited processing and a waiver of fees.

I. Documents Requested

This request seeks information about how the Massachusetts JTTF functions, how its authority is divided and shared, what safeguards are in place to ensure the civil liberties of those whom it targets, and the number and type of investigations conducted out of Massachusetts. The request also seeks specific information about the Massachusetts JTTF's involvement in the investigation into and death of a suspect, Ibragim Todashev. In particular, we respectfully request the following documents:

A. Structure of the Massachusetts JTTF

1. Records indicating the Massachusetts JTTF's purpose and organization, its membership and command structure, and its relationship with the Federal Bureau of

Investigation and the U.S. Attorney's Office for the District of Massachusetts.

2. Records indicating the number of FBI personnel assigned to the Massachusetts JTTF and, of that number, how many are (a) field agents or investigators, (b) intelligence analysts, or (c) support personnel.

3. Records identifying each federal, state, and local agency other than the FBI that participates in the Massachusetts JTTF, including records that show how many agents from each such agency are assigned to the Massachusetts JTTF.

4. All memoranda of understanding, contracts, or agreements between the Massachusetts JTTF and (a) any federal agency, (b) the Commonwealth of Massachusetts or any department, agency, authority, or official of the Commonwealth, and (c) any Massachusetts city or town or any department, agency, or official of a Massachusetts city or town addressing the assignment of personnel to the Massachusetts JTTF.

5. Records showing the number of Massachusetts JTTF personnel whose responsibilities require them to be physically present for any period of time at the Massachusetts Commonwealth Fusion Center or the Boston Regional Intelligence Center.

6. Records describing the structure of or protocols for information sharing between the Massachusetts JTTF and the Boston Regional Intelligence Center, the Commonwealth Fusion Center, the Massachusetts Bay Transportation Authority, or the Massachusetts Department of Transportation.

7. Documents showing the budget of the Massachusetts JTTF, including sources of funding from 2010 to present.

B. FBI Boston Field Office Investigations

1. All documents showing how many assessments, preliminary investigations, and full investigations the FBI Boston Field Office has conducted since 2011 and how many of those assessments/investigations led to arrests, prosecutions or convictions. If available, please provide records that break down the investigations by category, such as domestic/international terrorism, drugs, RICO, and gangs.

2. All documents showing, as of the date that the agency identifies the responsive records, the number of FBI investigations that are open, the number that are

assessments, preliminary investigations, and full investigations and the category of each open investigation.

C. Massachusetts JTTF involvement with Ibragim Todashev

1. All documents relating to Ibragim Todashev.

2. All documents relating to any investigation into the involvement of members of the Massachusetts JTTF in the death of Ibragim Todashev.

II. Request for expedited processing

ACLUM requests expedited processing under 5 U.S.C. § 552(a)(6) and 28 C.F.R. § 16.5(d). The FOIA statute and DOJ regulations allow for expedited processing when the records are urgently needed to inform the public about actual or alleged government activity and when the information relates to a matter of widespread media interest in which there exist questions about the government's integrity that affect public confidence. 5 U.S.C. § 552(a)(6); 28 C.F.R. § 16.5(d)(1)(ii) and (iv). Furthermore, ACLUM is an organization that regularly disseminates information that can help the public judge the government's integrity. In order to receive expedited processing for an issue of urgent concern, the requester must be "primarily engaged in disseminating information." *See* 28 C.F.R. §16.5(d)(1)(ii).

Those conditions are met here. There is an urgent need to inform the public about the workings of the Massachusetts JTTF, an issue that has been of widespread and exceptional media and public interest and raises questions about the government's integrity. Additionally, ACLUM is an organization primarily engaged in disseminating information.

A. There is an urgent need to inform the public about questions surrounding the Massachusetts JTTF.

There is an urgent need to inform the public about the subjects of this records request—namely, the organization and conduct of the Massachusetts JTTF, and its involvement in the investigation and death of Ibragim Todashev—because these records concern timely, newsworthy, and important questions about recent government conduct and overall government integrity. Moreover, very little information about these subjects is

otherwise available to the public. Thus, without the information sought, the public's ability to judge the actions of the Massachusetts JTTF could be severely impaired.

1. The Boston Marathon bombings and Ibragim Todashev

In the wake of the Boston Marathon bombings, cooperation between state and federal authorities has come under public scrutiny. Local news outlets, including *The Boston Globe* and *Boston Magazine*, have devoted considerable recent coverage to law enforcement and intelligence efforts following and preceding the bombings.[1] Soon after the bombings, reports surfaced that the FBI had received warnings about and had conducted an investigation into alleged bomber Tamerlan Tsarnaev, but had not shared that information with local agencies.[2] Former Boston Police Commissioner Ed Davis testified before Congress that a detective he had assigned to the JTTF was completely unaware of the investigation, adding to the public concerns about the functions of JTTFs.[3] At Congressional hearings, members of Congress and the media additionally expressed concern over the information-sharing relationship between federal law enforcement agencies and the state and local agencies.[4]

The lack of information surrounding the Massachusetts JTTF's involvement in the Boston Marathon bombing investigations has led to many unanswered questions and affected the public's confidence in federal-local law enforcement collaboration. Without

---

[1] *See, e.g.*, Susan Zalkind, *Coakley Hasn't Followed Through on Promise to Families of Waltham Triple-Murder Victims*, Boston Magazine, Oct. 3, 2013, *available at* http://www.bostonmagazine.com/news/blog/2013/10/03/martha-coakley-promise-waltham-triple-murder-victim-families/; Bryan Bender, *Keating Wants FBI to Offer Answers on Bombings,* The Boston Globe, July 31, 2013, *available at* http://www.bostonglobe.com/news/politics/2013/07/31/keating-demands-more-answers-from-new-fbi-chief-boston-bombings/lTFYR6jw5Sc7KG3N0wcnJP/story.html; Alicia A. Caldwell, *Ed Davis: Boston Police Not Told FBI Had Tamerlan Tsarnaev Warning*, May 9, 2013, http://boston.cbslocal.com/2013/05/09/ed-davis-to-testify-at-congressional-hearing-on-boston-marathon-bombings/.

[2] Joe Johns, *CNN's Q and A with FBI Director Robert Mueller*, CNN, Aug. 22, 2013, http://www.cnn.com/2013/08/22/politics/fbi-mueller-interview/?hpt=po_c2.

[3] Alicia A. Caldwell, *Ed Davis: Boston Police Not Told FBI Had Tamerlan Tsarnaev Warning*, May 9, 2013, http://boston.cbslocal.com/2013/05/09/ed-davis-to-testify-at-congressional-hearing-on-boston-marathon-bombings/.

[4] Matt Viser, *Tensions Emerge Over Lack of Tsarnaev Information Shared Between FBI, Local Authorities*, The Boston Globe, May 9, 2013, *available at* http://www.boston.com/politicalintelligence/2013/05/09/tensions-emerge-over-lack-tsarnaev-information-shared-between-fbi-local-authorities/c0JqORZNBkQJomxbODmwVK/story.html (reporting that the Boston JTTF has "representatives from the Boston Police Department").

disclosure of the records sought, the public will remain in the dark about the structure and operations of the Massachusetts JTTF's involvement in the actions surrounding the Boston Marathon bombings, and will not be able to assess whether the program is effective or subject to sufficient limits and oversight.

Specifically, the request seeks information relating to the Massachusetts JTTF's involvement in the death of Ibragim Todashev, an associate of alleged Boston Marathon bomber Tamerlan Tsarnaev. Mr. Todashev was shot and killed while being questioned by an FBI agent and two members of the Massachusetts State Police, who likely were members of the Massachusetts JTTF.[5] Todashev's death and his connection to an unsolved triple-murder in Waltham, Massachusetts—to which Tsarnaev has also been linked—has led to considerable media and public interest, and have left many open questions.[6]

2. *Inter-agency cooperation and the JTTFs*

In addition to lacking sufficient information about the Massachusetts JTTF's possible involvement in the Todashev investigation, the public also lacks sufficient information about the Massachusetts JTTF more generally. This public records request seeks to address that problem.

For more than two decades, the federal government has implemented or expanded programs that have enhanced coordination among federal, state and local law enforcement agencies. The Joint Terrorism Task Forces are a crucial part of this expansion. Created in some districts as early as 1990, the JTTFs' mission is to "detect and investigate terrorists and terrorist groups and prevent them from carrying out terrorist acts directed against the United States."[7] Operating from the FBI's field office, the JTTF has primary responsibility for terrorism investigations and is the "operational unit that conducts field investigations of actual or potential terrorism threats."[8]

Nationwide collaboration between the FBI and local law enforcement has been the subject of sustained media interest for several years and has led to questions about its

---

[5] Michael S. Schmidt, William K. Rashbaum and Richard A. Oppel Jr., *Deadly End to F.B.I. Queries on Tsarnaev and a Triple Killing*, N.Y. Times, May 22, 2013.

[6] *See, e.g.*, Zalkind, *supra* n.1; Hilary Sargent, *Asked and (un)answered: The Todashev saga continues.* Boston.com, Oct. 24. 2013, *available at* http://www.boston.com/blogs/news/local/chartgirl/2013/10/asked_and_unanswered_the_todashev_saga_continues.html.

[7] *The Department of Justice's Terrorism Task Forces,* U.S. Department of Justice, Office of the Inspector General, Evaluation and Inspections Division, Report No. I-2005-007, June 2005, http://www.justice.gov/oig/reports/plus/e0507/final.pdf (last accessed Nov. 26, 2013).

[8] *Id.*

breadth and effectiveness.[9] For example, the 2008 updates to the FBI's Domestic Investigations Operations Guidelines (DIOG) received much media attention.[10] The guidelines, which relaxed the requirements to open investigations on individuals and groups, relate directly to the functioning of the JTTFs. The *New York Times* recently reported that during 2009-2011, the bureau opened 82,325 assessments of people and groups searching for signs of wrongdoing.[11] Agents closed out most of the assessments without finding information that justified a more intensive inquiry. In 2011, the Massachusetts JTTF alone performed 1,000 assessments.[12]

The high number of assessments relative to the number that developed into more intensive investigations raises civil liberties concerns because the FBI retains the data it collects about targets, even if the investigation leads nowhere. Mike German, a former FBI agent who now works for the ACLU, said, "[t]hese are investigations against completely innocent people that are now bound up within the F.B.I.'s intelligence system forever. Is that the best way for the F.B.I. to use its resources?"[13] In contrast, others have criticized the lack of coordination between the Massachusetts JTTF and local law enforcement as creating a threat to public safety.[14]

Discussion of JTTFs has reached Congress as well. Government officials and non-governmental advocates have testified before numerous bodies of the U.S. Congress regarding the workings and effectiveness of the JTTFs and, more broadly, the sharing of information between local, state and federal agencies.[15]

---

[9] *See, e.g.*, Eric Schmitt, *Surveillance Effort Draws Civil Liberties Concern,* N.Y. Times, Apr. 28, 2009; Martine Powers, *Police Accused of Spying on Hub Antiwar Groups: No Links to Terror or Crime Apparent*, The Boston Globe, Oct. 18, 2012, at B1; Torin Monahan, "The Future of Security? Surveillance Operations at Homeland Sec. Fusion Centers," *Social Justice*, Vol. 37, No. 2, pg. 120, (2010).

[10] http://www.privacysos.org/sites/all/files/DIOG.pdf (last accessed Nov. 26, 2013). *See also* Kade Crockford, *The FBI can do what?!*, *Privacy SOS blog*, at http://privacysos.org/degraded_standards (last accessed Nov. 26, 2013).

[11] Charlie Savage, *F.B.I. Focusing on Security Over Ordinary Crime*, N.Y. Times, Aug. 23, 2011, at http://www.nytimes.com/2011/08/24/us/24fbi.html?_r=0.

[12] *See, e.g.*, Viser, *supra* n.4.

[13] Charlie Savage, *F.B.I. Casts Wide Net Under Relaxed Rules for Terror Inquiries, Data Show*, N.Y. Times, Mar. 26, 2011, at http://www.nytimes.com/2011/03/27/us/27fbi.html.

[14] *See, e.g.*, Viser, *supra* n.4 (reporting that the Boston JTTF has "representatives from the Boston Police Department").

[15] *See e.g., Eight Years After 9/11: Confronting Terrorist Threat to Homeland: Hearing Before Senate Comm. On Homeland Security,* 111th Cong. (Oct. 1, 2009) (testimony of Janet Napolitano, Sec. Dep't of Homeland Security); *Strategies for Terrorism Information Sharing, Hearing Before Senate Judiciary Comm.*, 111th Cong. (Apr. 21, 2009) (testimony of Caroline Frederickson, Director, ACLU Washington Legislative Office); Robert O'Harrow Jr., *DHS 'Fusion Centers' Portrayed as Pools of*

Despite public questions as to the effectiveness of the JTTFs, the task forces operate largely in secret. Little is known about their basic mechanics, their cost, the number and type of investigations they perform, or their track record. This request seeks documents that can inform public debate about this significant government program.

B. ACLUM is "primarily engaged in disseminating information."

In order to receive expedited processing for an issue of urgent concern, the requester must be "primarily engaged in disseminating information." 28 C.F.R. §16.5(d)(1)(ii). Gathering and disseminating current information to the public is a critical and substantial component of ACLUM's mission and work.

ACLUM, a non-profit, non-partisan organization with over 18,000 members and supporters across Massachusetts is dedicated to the principles of liberty and equality. As the Massachusetts affiliate of the national ACLU, a non-profit, non-partisan organization with over 500,000 members nationwide, ACLUM distributes information within and outside of Massachusetts.

ACLUM publishes newsletters, news briefings, reports and other materials that are disseminated to the public.[16] These materials are widely available to everyone, including tax-exempt organizations, journalists, students, faculty, and other interested individuals at no cost. ACLUM also disseminates information through its website (www.aclum.org), a widely read blog (http://www.privacysos.org), posts on social media sites such as Facebook and Twitter, and public speaking engagements.[17] ACLUM's web postings address civil liberties issues in depth, provide features on civil liberties issues in the news, and contain hundreds of documents that relate to the issues addressed by ACLUM, including features on information obtained through public records.[18]

The national ACLU also publishes, analyzes, and disseminates information through its heavily visited website, www.aclu.org. The website serves as a clearinghouse for news about ACLU issues, as well as analysis about case developments, and an archive of case-related documents. Through these pages, the ACLU provides the public with educational

---

Ineptitude, Civil Liberties Intrusions, Wash. Post, Oct. 2, 2012; James Risen, *Criticism of Centers in Fight on Terror*, N.Y. Times, Oct. 3, 2012, at A17; Shaun Waterman, *Lawmakers: FBI Stonewalling on Tsarnaev*, Wash. Times, Jul. 11, 2013; Michael T. McCaul & Peter T. King, *Majority Staff Report on The National Network of Fusion Centers*, H.R. Comm. on Homeland Sec., July, 2013.

[16] *See* Exhibits 1-4.

[17] *See* Exhibits 5-11.

[18] *See, e.g.*, www.aclum.org/policing_dissent; www.aclum.org/ice.

material about civil liberties issues, recent news about related issues, analyses of Congressional or executive branch action, government documents obtained through FOIA, and in-depth analytic and educational multi-media features.[19]

An example of an ACLU feature on information obtained through the FOIA is the "Torture FOIA" webpage, https://www.aclu.org/accountability-torture, which contains commentary about the ACLU's FOIA request relating to the treatment of prisoners in Afghanistan, Guantanamo and Iraq, analysis of the documents released by the government, press releases, and an advanced search engine that allows interested individuals to sift through the 100,000 pages of documents obtained through FOIA.

Courts have found organizations with similar missions and information-dissemination activities to be "primarily engaged in disseminating information." *See, e.g., Electronic Frontier Foundation v. Office of the Director of Nat. Intelligence,* 542 F. Supp. 2d 1181, 1183 (N.D. Cal. 2008) (Electronic Frontier Foundation); *Leadership Conference on Civil Rights v. Gonzales,* 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (Leadership Conference on Civil Rights); *ACLU v. Dep't of Justice,* 321 F. Supp. 2d at 30 n.5 (D.D.C. 2004) (Electronic Privacy Information Center).

ACLUM plans to analyze and disseminate to the public the information gathered through this request at no cost.

III. Application for a Waiver or Limitation of Fees

ACLUM is entitled to a fee waiver or limitation of fees under the FOIA statute and Department of Justice Regulations for two reasons. First, release of the records requested is in the public interest and not in any commercial interest of the requester. U.S.C. § 552 (4)(A)(iii); 28 CFR § 16.11(k)(1)(i) and (ii). Second, the requester qualifies as a

---

[19] For example, the ACLU's website about national security letters ("NSLs") includes: an explanation of what NSLs are; information about and document repositories for the ACLU's NSL cases; links to documents obtained through FOIA about various agencies' use of NSLs; NSL news in the courts, Congress, and executive agencies; links to commentary on NSL-related news; educational web features about the NSL gag power; public education reports about NSLs and the Patriot Act; news about and analysis of the Department of Justice Inspector General's reviews of the FBI's use of NSLs; the ACLU's policy analysis and recommendations for reform of the NSL power; charts with analyzed data about the government's use of NSL; myths and facts documents; and links to information and analysis of related issues. *See* https://www.aclu.org/national-security-technology-and-liberty/national-security-letters.

representative of the news media. 5 U.S.C. § 552(a)(4)(A)(ii)(III); 28 C.F.R. § 16.11(a)(b)(1)(6).

A. The release of records is in the public interest.

Under the FOIA statute and DOJ regulations, documents shall be provided free of charge or at a reduced rate if the information sought is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and the information is not primarily in the commercial interest of the requester. 5 U.S.C. § 552 (4)(A)(iii); 28 CFR § 16.11(k)(1)(i) and (ii).

This request aims at furthering the public's understanding of government activity, namely the workings of the Massachusetts JTTF. As discussed above, there is substantial media and public interest in the workings of the MA JTTF, yet little information is publicly available. *See supra* Part II.A. The release of the requested records would provide previously-unknown information that would allow the public to better debate this important government function.

Moreover, as a non-profit organization, ACLUM has no commercial interest in the information sought. In the past, ACLUM and the national ACLU have disclosed documents obtained through FOIA free of charge and without limits.[20] Any information obtained as a result of this FOIA request will be made available to the public at no cost. Thus, a fee waiver would fulfill Congress's legislative intent in amending FOIA. *See Judicial Watch Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) ("Congress amended FOIA to ensure that it be 'liberally construed in favor of waivers for noncommercial requesters.'" (citation omitted)); OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524, § 2 (Dec. 31, 2007) (finding that "disclosure, not secrecy, is the dominant objective of the Act").

B. ACLUM is a "representative of the news media" as defined in the statute and regulations.

Under FOIA and DOJ regulations, search and review fees shall not be charged to "representatives of the news media" 5 U.S.C. § 552(a)(4)(A)(ii)(II); 28 C.F.R. § 16.11(d)(1). ACLUM meets the statutory and regulatory definitions of a "representative of the news media" because it "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii)(III); *see also Nat'l Sec. Archive v. Dep't of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); *cf. ACLU v. Dep't of Justice*, 321 F. Supp. 2d at 30 n.5

[20] *See, e.g.*, www.aclum.org/ice; www.aclum.org/alpr.

(finding the non-profit public interest group to be "primarily engaged in disseminating information").

ACLUM is a "representative of the news media" for the same reasons it is "primarily engaged in the dissemination of information." *See Elec. Privacy Info. Ctr. v. Dep't of Def.*, 241 F. Supp. 2d 5, 10-15 (D.D.C. 2003) (finding non-profit public interest group that disseminated an electronic newsletter and published books was a "representative of the media" for purposes of FOIA). ACLUM disseminates information through many channels, including its websites, blogs, press releases, reports, newsletters, news briefings, fact sheets, educational brochures, pamphlets, television series, and public speaking engagements. *See supra*, part II.B. As Senator Leahy said during a debate about FOIA's fee-waiving provisions: "[A]ny person or organization which regularly publishes or disseminates information to the public . . . should qualify for waivers as a 'representative of the news media.'" 132 Cong. Rec. S14292 (daily ed. Sept. 30, 1986).

On account of the factors discussed above, agencies such as DHS, DOJ and TSA have recently waived fees for ACLUM requests. For example, citing ACLUM's statement that it would disseminate to the public certain records requested from the FBI, the Section Chief of the FBI's Records/Information Dissemination Section granted ACLUM a fee waiver in 2012.[21] Similarly, the national ACLU and other state ACLU affiliates regularly receive fee waivers on account of these factors.[22]

---

[21] See Exhibit 12

[22] See Exhibit 13. For example, June 2011 (National Security Division of the Department of Justice); October 2010 (Department of the Navy); January 2009 (CIA); March 2009 (State Department); December 2008 (Department of Justice); November 2006 (Department of Health and Human Services); May 2005 (United States Department of Commerce); March 2005, April 2007, June 2006, February 2006, October 2003 (Department of State). Lastly, the ACLU of Washington recently was held to be a "representative of the news media." *ACLU of Wash. v. Dep't of Justice*, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011).

IV. Conclusion

We look forward to your reply to the Request within twenty (20) business days, as required under 5 U.S.C. § 552(a)(6)(A)(i).

Thank you for your prompt attention to this matter.

Sincerely,

Laura Rótolo
ACLU of Massachusetts
211 Congress Street
Boston, MA 02110

Laura E. Deck
Proskauer Rose LLP
One International Place
Boston, MA 02110

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

AMERICAN CIVIL LIBERTIES UNION OF MASSACHUSETTS, Plaintiff, v. DEPARTMENT OF JUSTICE, *et al.*, Defendants.	Civ. A. No. 14-11759-ADB

SECOND DECLARATION OF DAVID M. HARDY

I, David M. Hardy, declare as follows:

(1) I am the Section Chief of the Record/Information Dissemination Section ("RIDS"), Records Management Division ("RMD"), in Winchester, Virginia. I have held this position since August 1, 2002. Prior to my joining the Federal Bureau of Investigation ("FBI"), from May 1, 2001 to July 31, 2002, I was the Assistant Judge Advocate General of the Navy for Civil Law. In that capacity, I had direct oversight of Freedom of Information Act ("FOIA") policy, procedures, appeals, and litigation for the Navy. From October 1, 1980 to April 30, 2001, I served as a Navy Judge Advocate at various commands and routinely worked with FOIA matters. I am also an attorney who has been licensed to practice law in the State of Texas since 1980.

(2) In my official capacity as Section Chief of RIDS, I supervise approximately 248 employees who staff a total of ten (10) Federal Bureau of Investigation Headquarters ("FBIHQ") units and two (2) field operational service center units whose collective mission is to effectively

plan, develop, direct, and manage responses to requests for access to FBI records and information pursuant to the FOIA as amended by the OPEN Government Act of 2007, the OPEN FOIA Act of 2009 and the FOIA Improvement Act of 2016; the Privacy Act of 1974; Executive Order 13526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and Presidential and Congressional directives. My responsibilities also include the review of FBI information for classification purposes as mandated by Executive Order 13526, and the preparation of declarations in support of Exemption 1 claims asserted under the FOIA. I have been designated by the Attorney General of the United States as an original classification authority and a declassification authority pursuant to Executive Order 13526, §§ 1.3 and 3.1. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

(3) Due to the nature of my official duties, I am familiar with the procedures followed by the FBI in responding to Plaintiff's request for information from its files pursuant to the provisions of the FOIA, 5 U.S.C. § 552. Specifically, I am aware of the FBI's handling of Plaintiff's FOIA request for the Massachusetts Joint Terrorism Task Force ("JTTF") involvement with Ibragim Todashev.

(4) This declaration is submitted in support of the FBI's Motion for Summary Judgment. It incorporates by reference my previous declaration dated July 24, 2015 (hereinafter "First Hardy Declaration") (Dkt. No. 53), documents the FBI's review of responsive documents, and justifies the FBI's assertion of FOIA Exemption (b)(7)(A) to categorically withhold records responsive to Plaintiff's request relating to Ibrahim Todashev. In addition, the FBI processed a

total of 1,148[1] responsive pages. Of these pages, 378 pages were released in full, 418 pages released in part, and 352 pages were withheld in full[2]. In accordance with Vaughn v. Rosen, 484 F.2d 820 (D.C. Cir. 1973), this declaration provides the Court and Plaintiff with the procedures used to search for, review, and process the responsive records, and of the FBI's justification for withholding certain records in full or in part pursuant to FOIA Exemptions (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(A), (b)(7)(C), (b)(7)(D), and (b)(7)(E).

ADMINISTRATIVE HISTORY OF PLAINTIFF'S FOIA REQUEST

(5) By letter dated December 9, 2013, Plaintiff submitted a FOIA request to the FBI seeking access to records on the structure of the Massachusetts JTTF including:

1. Records indicating the Massachusetts JTTF's purpose and organization, its membership and command structure, and its relationship with the Federal Bureau of Investigation and the U.S. Attorney's Office for the District of Massachusetts.
2. Records indicating the number of FBI personnel assigned to the Massachusetts JTTF and, of that number, how many are (a) field agents or investigators, (b) intelligence analyst, or (c) support personnel.
3. Records identifying each federal, state, and local agency other than the FBI that participates in the Massachusetts JTTF, including records that show how many agents from each such agency are assigned to the Massachusetts JTTF.

---

[1] The FBI inadvertently skipped a bates page when stamping the documents; therefore, there are only 1,148 total pages reviewed, but the releases are bates stamped Todashev-1 to Todashev-1149. There are no missing responsive pages.

[2] Of these, approximately 46 pages were withheld in full as duplicative of other pages.

4. All memoranda of understanding, contracts, or agreements between the Massachusetts JTTF and (a) any federal agency, (b) the Commonwealth of Massachusetts or any department, agency, authority, or official of the Commonwealth, and (c) any Massachusetts city or town or any department, agency, or official of a Massachusetts city or town addressing the assignment of personnel to the Massachusetts JTTF.
5. Records showing the number of Massachusetts JTTF personnel whose responsibilities require them to be physically present for any period of time at the Massachusetts Commonwealth Fusion Center or the Boston Intelligence Center.
6. Records describing the structure of or protocols for information sharing between the Massachusetts JITF and the Boston Regional Intelligence Center, the Commonwealth Fusion Center, the Massachusetts Bay Transportation Authority, or the Massachusetts Department of Transportation.
7. Documents showing the budget of the Massachusetts JTTF, including sources of funding from 2010 to present.

Plaintiff also sought records concerning FBI Boston Field Office Investigations, including:

1. All documents showing how many assessments, preliminary investigations, and full investigations the FBI Boston Field Office has conducted since 2011 and how many of those assessments/investigations led to arrests, prosecutions or convictions. If available, please provide records that break down the

investigations by category, such as domestic/international, drugs, RICO, and gangs.

2. All documents showing, as of the date that the agency identifies the responsive records, the number of FBI investigations that are open, the number that are assessments, preliminary investigations, and full investigations and the category of each open investigation.

Plaintiff also sought records pertaining to Massachusetts JTTF involvement with Ibragim Todashev, including:

1. All documents relating to Ibragim Todashev.
2. All documents relating to any investigation into the involvement of members of the Massachusetts JTTF in the death of Ibragim Todashev.

Finally, Plaintiff requested expedited processing and a fee waiver. **(*See* Exhibit A.)**

(6) For administrative convenience, the FBI opened three separate cases in its FOIPA Document Processing System ("FDPS").[3] FOIA request Number 1246012 addressed the part of the request pertaining to records on the structure of the Massachusetts JTTF, FOIA Request Number 1246014 addressed Plaintiff's request for records pertaining to the FBI Boston Field Office Investigations, and FOIA Request Number 1246017 addressed Plaintiff's request for records pertaining to Ibragim Todashev. The First Hardy Declaration addressed FOIA Numbers 1246012 and 1246014. This declaration addresses FOIA Request Number 1246017 pertaining to Ibragim Todashev.

---

[3] FDPS is the internal repository and application utilized by RIDS to process, track, and respond to FOIA and or Privacy Act ("FOIA/PA") requests received by FBI. It stores FOIPA related records.

FOIPA Request Number 1246017-000

(7) By letter dated January 2, 2014, the FBI acknowledged receipt of Plaintiff's request and assigned it FOIA Request Numbers 1246017. The FBI advised Plaintiff it was searching the indices to the Central Records System for information responsive to its request. The FBI further advised that Plaintiff's request for a fee waiver was being considered and that it will be advised of the decision at a later date. ***(See* Exhibit B.)**

(8) By letter dated January 14, 2014, the FBI advised Plaintiff that the material requested was located in an investigative file which was exempt from disclosure pursuant to 5 U.S.C. § 552(b)(7)(A) because there was a pending or prospective law enforcement proceeding relevant to these records and release of the information could reasonably be expected to interfere with the enforcement proceedings. The FBI advised Plaintiff that it could appeal the FBI's determination by filing an administrative appeal with the Department of Justice ("DOJ"), Office of Information Policy ("OIP") within sixty (60) days from the date of its letter. **(*See* Exhibit C.)**

(9) By letter dated March 12, 2014, Plaintiff submitted an appeal to OIP contesting the FBI's January 14, 2014 response. **(*See* Exhibit D.)**

(10) By letter dated March 27, 2014, OIP acknowledged receipt of Plaintiff's appeal and assigned it appeal number AP-2014-01950. **(*See* Exhibit E.)**

(11) By letter dated April 30, 2014, OIP affirmed the FBI's (b)(7)(A) response to Plaintiff. **(*See* Exhibit F.)**

FOIPA Request Number 1246017-001

(12) On April 10, 2014, Plaintiff filed its complaint in the instant action. **(*See* Docket Number 1.)**

(13) By letter dated May 1, 2015, the FBI made its first interim release of records to Plaintiff. The FBI advised that 487 pages of records were reviewed and 247 pages of records were being released in full or part, with certain information withheld pursuant to FOIA Exemptions 1, 3, 6, 7C, 7D, 7E, and 9[4]. The FBI advised Plaintiff he could appeal the FBI's determination by filing an administrative appeal with OIP within sixty (60) days. **(*See* Exhibit G.)**

(14) By letter dated June 1, 2015, the FBI made its second and final release of records to Plaintiff. The FBI advised that 661 pages of records were reviewed and 532 pages of records were being released in full or part, with certain information withheld pursuant to FOIA Exemptions 1, 3, 5, 6, 7A, 7C, and 7E. The FBI advised Plaintiff he could appeal the FBI's determination by filing an administrative appeal with OIP within sixty (60) days. **(*See* Exhibit H.)**

(15) By letter dated May 15, 2017, the FBI re-released all of the processed responsive records with exemption codes. The FBI advised that 1,148[5] pages of records were reviewed and 796 pages of records were being released in full or part, with certain information withheld pursuant to FOIA Exemptions (b)(1), (b)(3), (b)(6), (b)(7)(C), and (b)(7)(E). The FBI also advised Plaintiff he could appeal the FBI's determination by filing an administrative appeal with OIP within ninety (90) days. **(*See* Exhibit I.)**

THE FBI'S CENTRAL RECORDS SYSTEM

[4] The FBI inadvertently cited FOIA Exemption 9 for this release. There was no information redacted using this FOIA exemption.

[5] *See* fn. 1, *supra.*

(16) The Central Records System ("CRS") is an extensive system of records consisting of applicant, investigative, intelligence, personnel, administrative, and general files compiled and maintained by the FBI in the course of fulfilling its integrated missions and functions as a law enforcement, counterterrorism, and intelligence agency to include performance of administrative and personnel functions. The CRS spans the entire FBI organization and encompasses the records of FBI Headquarters ("FBIHQ"), FBI Field Offices, and FBI Legal Attaché Offices ("Legats") worldwide.

(17) The CRS consists of a numerical sequence of files, called FBI "classifications," which are organized according to designated subject categories. The broad array of CRS file classification categories include types of criminal conduct and investigations conducted by the FBI, as well as categorical subjects pertaining to counterterrorism, intelligence, counterintelligence, personnel, and administrative matters. For identification and retrieval purposes across the FBI, when a case file is opened, it is assigned a Universal Case File Number ("UCFN") consisting of three sequential components: (a) the CRS file classification number, (b) the abbreviation of the FBI Office of Origin ("OO") initiating the file, and (c) the assigned individual case file number for that particular subject matter.[6] Within each case file, pertinent documents of interest are "serialized," or assigned a document number in the order which the document is added to the file, typically in chronological order.

THE CRS GENERAL INDICES AND INDEXING

[6] For example, in a fictitious file number of "11Z-HQ-56789;" the "11Z" component indicates the file classification, "HQ" indicates that FBI Headquarters is the FBI OO of the file, and "56789"is the assigned case specific file number.

(18) The general indices to the CRS are the index or "key" to locating records within the enormous amount of information contained in the CRS. The CRS is indexed in a manner which meets the FBI's investigative needs and priorities, and allows FBI personnel to reasonably and adequately locate pertinent files in the performance of their law enforcement duties. The general indices are arranged in alphabetical order and comprise an index on a variety of subject matters to include individuals, organizations, events, or other subjects of investigative interest that are indexed for future retrieval. The entries in the general indices fall into two category types:

a. Main entry. This entry pertains to records indexed to the main subject(s) of a file, known as "main file" records. The "main" entry carries the name of an individual, organization, or other subject matter that is the designated subject of the file.

b. Reference entry. This entry, or a "cross-reference," pertains to records that merely mention or reference an individual, organization, or other subject matter that is contained in a "main" file record about a different subject matter.

(19) FBI employees may index information in the CRS by individual (persons), by organization (organizational entities, places, and things), and by event (*e.g.,* a terrorist attack or bank robbery). Indexing information in the CRS is based on operational necessity, and the FBI only indexes that information considered relevant and necessary for future retrieval. Accordingly, the FBI does not index every individual name or other subject matter in the general indices.

AUTOMATED CASE SUPPORT

(20) Automated Case Support ("ACS") is an electronic, integrated case management system that became effective for FBIHQ and all FBI Field Offices and Legats on October 1, 1995. As part of the ACS implementation process, over 105 million CRS records were

converted from automated systems previously utilized by the FBI into a single, consolidated case management system accessible by all FBI offices. ACS has an operational purpose and design to enable the FBI to locate, retrieve, and maintain information in its files in the performance of its myriad missions and functions.[7]

(21) The Universal Index ("UNI") is the automated index of the CRS and provides all offices of the FBI a centralized, electronic means of indexing pertinent investigative information to FBI files for future retrieval via index searching. Individual names may be recorded with applicable identifying information such as date of birth, race, sex, locality, Social Security Number, address, and/or date of an event. Moreover, ACS implementation built upon and incorporated prior automated FBI indices; therefore, a search employing the UNI application of ACS encompasses data that was already indexed into the prior automated systems superseded by ACS. As such, a UNI index search in ACS is capable of locating FBI records created before its 1995 FBI-wide implementation to the present day in both paper and electronic format.[8] Currently, UNI consists of approximately 116.1 million searchable records and is updated daily with newly indexed material.

ACS and SENTINEL

[7] ACS and the next generation Sentinel system are relied upon by the FBI daily to fulfill essential functions such as conducting criminal, counterterrorism, and national security investigations; background investigations; citizenship and employment queries, and security screening, to include Presidential protection.

[8] Older CRS records that were not indexed into UNI as a result of the 1995 ACS consolidation remain searchable by manual review of index cards, known as the "manual indices." A search of the manual indices is triggered for requests on individuals if the person was born on or before January 1, 1958; and for requests seeking information about organizations or events on or before January 1, 1973. Records created after these dates would be captured through a UNI search.

(22) Sentinel is the FBI's next generation case management system that became effective FBI-wide on July 1, 2012. Sentinel provides a web-based interface to FBI users, and it includes the same automated applications that are utilized in ACS. After July 1, 2012, all FBI generated records are created electronically in case files via Sentinel; however, Sentinel did not replace ACS and its relevance as an important FBI search mechanism. Just as pertinent information was indexed into UNI for records generated in ACS before July 1, 2012, when a record is generated in Sentinel, information is indexed for future retrieval. Moreover, there is an index data sharing nexus between the Sentinel and ACS systems whereby components of information indexed into Sentinel are also replicated or "backfilled" into ACS. In sum, the Sentinel case management system builds on ACS and shares its operational purpose; Sentinel provides another portal to locate information within the vast CRS for FBI records generated on or after July 1, 2012.

SEARCH FOR RECORDS RESPONSIVE TO PLAINTIFF'S FOIA REQUESTS

FOIA REQUEST NO. 1246017

(23) Following receipt of this FOIA request, the FBI conducted a search of the ACS in order to locate records responsive to Ibragim Todashev. The FBI conducted this search utilizing a three-way phonetic[9] breakdown of "Ibragim Todashev" to include the variation "I Todashev."

[9] Three-way phonetic search ("TP" search) – the FBI used the phonetic search capabilities of ACS to conduct a TP search of subject's name. This means that first, the computer automatically broke the three names down, searching the index for different name variations of those entered: "I Todashev," "Ibragim Abdulbakiyevich Todashev," "Ibrahim Todashev." Then, the computer breaks names down based on their phonetic characteristics. The computer will return results based on whether or not they phonetically match a certain percentage of the first and last names searched.

Through this search, the FBI located a closed Tampa FBI Field Office file pertaining to the FBI's investigation into the shooting death of Ibragim Todashev by an FBI Special Agent ("SA"), 89B-TP-2886360 processed here. Additionally, the FBI located one pending FBI Tampa Field Office main file and numerous serials and one sub-file located within pending Boston Field Office investigative files, all pertaining to Ibragim Todashev. These pending serials include numerous serials from the Boston Field Office Boston Marathon Bombing investigation as well as four cross-references and one sub-file from three different Boston Field Office investigations related to the Boston Marathon Bombing. These pending files continue to be pending and therefore are exempt in their entirety pursuant to FOIA Exemption 7(A).

(24) Additionally, following RIDS' correspondence with FBI's Inspection Division ("INSD") concerning the status of the FBI's investigation into the shooting death if Ibragim Todashev, INSD provided RIDS with additional responsive serials from INSD files 297-HQ-A1271699-D and 297-HQ-A1271966-D.

(25) Scope of Search. RIDS conducted a search of all files within the CRS reasonably calculated to locate records responsive to Plaintiff's request. First, given its comprehensive nature and scope, the CRS is the principal records system searched by RIDS, to locate information responsive to most FOIPA requests, because the CRS is where the FBI indexes information about individuals, organizations, events, and other subjects of investigative interest for future retrieval. Second, given Plaintiff's request seeks information about Ibragim Todashev, such information would reasonably be expected to be located in the CRS via the index search methodology the FBI employed here.

JUSTIFICATION FOR NONDISCLOSURE UNDER THE FOIA

(26) The paragraphs that follow explain the FBI's basis for withholding information within the responsive records. Part I provides justifications for specific exemption categories asserted within records that were processed and released, as well as within some records withheld in full. See ¶¶ 27-133, *infra*. Part II provides justification applicable only to the records withheld in full pursuant to FOIA Exemption (b)(7)(A)[10] *See* ¶¶ 134-140C, *infra*.

(27) All documents responsive to Plaintiff's request were processed to achieve maximum disclosure consistent with the access provisions of the FOIA. Every effort was made to provide Plaintiff with all material in the public domain and with all reasonably segregable, non-exempt information in the responsive records. No reasonably segregable, nonexempt portions have been withheld from Plaintiff. Further description of the information withheld, beyond what is provided in this declaration could identify the actual exempt information that the FBI has protected. Copies of the pages released in part and in full have been consecutively numbered "Todashev-1 through Todashev-1149[11]" at the bottom of each page. Pages withheld in their entirety (*e.g.*, removed per exemption or duplicates) were replaced by a "Deleted Page Information Sheet" ("DPIS"), which identifies the reason and/or the applicable FOIA exemptions relied upon to withhold the page in full, as well as the Bates numbers for the withheld material. The DPISs and Bates-numbered pages that were withheld in part have been provided to Plaintiff by letters dated May 1, 2015, June 1, 2015, and May 15, 2017; and will be made available to the Court upon request. *See* ¶¶ 13-15, *supra*. The exemptions asserted by the FBI as grounds for

---

[10] Pursuant to Maydak v. U.S. Department of Justice, 218 F. 3d 760 (D.C. Cir. 2000), the FBI also explains its reasoning for applying underlying exemptions to the records withheld in full pursuant to FOIA Exemption (b)(7)(A)

[11] *See* fn. 1, *supra.*

non-disclosure of portions of documents are Exemptions (b)(1), (b)(3), (b)(6), (b)(7)(A), (b)(7)(C), and (b)(7)(E).

PART I

Explanation of the Coded Format Used to Describe and Justify Withholdings

(28) The Bates-numbered documents contain, on their faces, coded categories of exemptions that detail the nature of the information withheld pursuant to the provisions of the FOIA. The coded categories are provided to aid the Court's and Plaintiff's review of the FBI's explanations of the FOIA exemptions it has asserted to withhold the material. The coded, Bates-numbered pages together with this declaration demonstrate that all material withheld by the FBI is exempt from disclosure pursuant to the cited FOIA exemptions, or is so intertwined with protected material that segregation is not possible without revealing the underlying protected material.

(29) Each instance of information withheld on the Bates-numbered documents is accompanied by a coded designation that corresponds to the categories listed below. For example, if "(b)(7)(C)-1" appears on a document, the "(b)(7)(C)" designation refers to FOIA Exemption 7(C) protecting against unwarranted invasions of personal privacy. The numerical designation of "1" following the "(b)(7)(C)" narrows the main category into a more specific subcategory, such as "Names and/or Identifying Information of FBI Special Agents/Support Personnel."

(30) Listed below are the categories used to explain the FOIA exemptions asserted to withhold the protected material in Part I. Many of these categories are duplicative of those described in the First Hardy Declaration at ¶ 24:

SUMMARY OF JUSTIFICATION CATEGORIES[12]	
CODED CATEGORIES	**INFORMATION WITHHELD**
Category (b)(1)	**CLASSIFIED INFORMATION**
(b)(1)-1	Intelligence Activities, Sources, and Methods (E.O. 13526 § 1.4(c)) [cited in conjunction with (b)(3)-1]
Category (b)(3)	**INFORMATION PROTECTED BY STATUTE**
(b)(3)-1	NSA of 1947 [50 USC Section 3024(i)(1)] [cited in conjunction with (b)(1)-1
Category (b)(6) and (b)(7)(C)	**CLEARLY UNWARRANTED INVASION OF PRIVACY AND UNWARRANTED INVASION OF PERSONAL PRIVACY**
(b)(6)-1 and (b)(7)(C)-1	Names and/or Identifying Information of FBI Special Agents/Support Personnel
(b)(6)-2 and (b)(7)(C)-2	Names and/or Identifying Information of Local Law Enforcement Personnel
(b)(6)-3 and (b)(7)(C)-3	Names and/or Identifying Data of Third Parties of Investigative Interest
(b)(6)-4 and (b)(7)(C)-4	Names of Non-FBI Federal Government Personnel and Foreign Law Enforcement or Intelligence Agency Personnel
(b)(6)-5 and (b)(7)(C)-5	Names and/or Identifying Information of Third Parties Merely Mentioned
Category (b)(7)(A)	**PENDING LAW ENFORCEMENT PROCEEDINGS**
(b)(7)(A)-1	Information Which, if Disclosed, Could Reasonably be Expected to Interfere with Pending Law Enforcement Proceedings
Category (b)(7)(E)[13]	**INVESTIGATIVE TECHNIQUES AND PROCEDURES**
(b)(7)(E)-2	FBI Internal Non-Public Intranet Web Addresses
(b)(7)(E)-3	Sensitive FBI Squads and/or Units
(b)(7)(E)-5	Sensitive FBI File Numbers and Descriptions
(b)(7)(E)-6	Collection / Analysis of Information
(b)(7)(E)-7	Operational Directives

EXEMPTION 1 – CLASSIFIED INFORMATION

[12] In the following paragraphs, there are several exemption categories that are not listed on this chart. These categories apply only to records withheld in full pursuant to b7A. These categories were not "coded" as such on the documents, since the documents are categorically denied.

[13] The FBI initially cited Categories (b)(7)(E)-1 & 4; however, these two categories are not used within the processed records at issue here in Part I.

(31) Exemption 1 protects records that are "(A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy; and (B) are in fact properly classified pursuant to such Executive Order . . . ." *See* 5 U.S.C. § 552(b)(1).

(32) Before I consider an Exemption (b)(1) claim for withholding agency records, I determine whether the information in those records is information that is currently and properly classified – *i.e.*, satisfies the requirements of Executive Order ("E.O.") 13,526 and complies with the various substantive and procedural criteria of the E.O. The E.O. 13,526 was signed by President Barack Obama on December 29, 2009, and is the Executive Order that currently governs the classification and protection of national security information.[14] I am bound by the requirements of E.O. 13,526 when making classification determinations.

(33) For information to be properly classified, and thus properly withheld from disclosure pursuant to Exemption 1, the information must meet the requirements set forth in E.O. 13,526 § 1.1(a):

(1) an original classification authority must have classified the information;

(2) the information must be owned by, produced by or for, or be under the control of the United States Government;

(3) the information must fall within one or more of the categories of information listed E.O. 13,526 § 1.4; and

(4) the original classification authority must determine that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against

[14] E.O. 13,526 § 6.1(cc) defines "National Security" as "the national defense or foreign relations of the United States."

transnational terrorism, and the original classification authority must be able to identify or describe the damage

(34) In addition to these substantive requirements, E.O. 13,526 sets forth certain procedural and administrative requirements that must be followed before information can be considered to be properly classified. Those requirements include the following:

(1) Each document must be marked as required and stamped with the proper classification designation.

(2) Each document must be marked to indicate clearly which portions are classified and which portions are exempt from declassification as set forth in E.O. 13,526 § 1.5(b).

(3) The prohibitions and limitations on classification specified in E.O. 13,526 § 1.7 were adhered to.

(4) The declassification policies set forth in E.O. 13,526 §§ 3.1 and 3.3 were followed.

(5) Any reasonably segregable portion of the classified documents that did not meet the standards for classification under E.O. 13,526 were declassified and marked for release, unless withholding was otherwise warranted under applicable law.

(35) All information which I determined to be classified was marked at the "Secret" level, since the unauthorized disclosure of this information reasonably could be expected to cause serious damage to national security.

Findings of the Declarant Regarding Exemption 1

(36) With the above requirements in mind, I personally and independently examined the information withheld from Plaintiff pursuant to FOIA Exemption 1 and determined that it is currently and properly classified pursuant to E.O. 13,526.

(37) I determined that this information satisfies the substantive requirements of the Executive Order. Specifically, I determined that the classified information protected by the FBI in this case is owned by, was produced by or for, and is under the control of the U.S.

Government, and that it was classified by an original classification authority. I further determined that the classified information protected by the FBI in this case continues to warrant classification at the "Secret" level (as marked on the documents) to protect "foreign government information" pursuant to E.O. 13,526 § 1.4(b); intelligence sources or methods, or cryptology" pursuant to E.O. 13,526 § 1.4(c); and information about "foreign relations or foreign activities of the United States, including confidential sources" pursuant to E.O. 13,526 § 1.4(d).

(38) Finally, I made certain that all procedural requirements of E.O. 13,526 set forth above were followed in order to ensure that the information was properly classified.

E.O. 13,526 § 1.4(b) – Foreign Government Information[15]

(39) E.O. 13,526 § 1.4(b) authorizes the classification of foreign government information. Foreign government information is defined as: "(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; (2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or (3) information received and treated as 'foreign government information' under the terms of a predecessor order." E.O. 13526, § 6.1(s)

[15] The FBI applied Exemption 1 to protect this type of information only within the categorically denied records within Part II.

(40) Many foreign governments do not officially acknowledge the existence of some of their intelligence and security services, or the scope of their activities or the sensitive information generated by them. The free exchange of information between United States intelligence and law enforcement services and their foreign counterparts is predicated upon the understanding that these liaisons, and information exchanged between them, must be kept in confidence.

(41) The release of official United States Government documents showing the existence of a confidential relationship with a foreign government reasonably could be expected to strain relations between the United States and the foreign governments and lead to diplomatic, political, or economic retaliations. A breach of this relationship can be expected to have at least a chilling effect on the free flow of vital information to the United States intelligence and law enforcement agencies, which may substantially reduce their effectiveness. Although the confidential relationship of the United States with certain countries may be widely reported, they are not officially acknowledged.

(42) Disclosure of such a relationship predictably will result in the careful analysis and possible compromise of the information by hostile intelligence services. The hostile service may be able to uncover friendly foreign intelligence gathering operations directed against it or its allies. This could lead to the neutralization of friendly allied intelligence activities or methods or the death of live sources, cause embarrassment to the supplier of the information, or result in economic or diplomatic retaliation against both the United States and the supplier of the information.

(43) Even if the government from which certain information is received is not named in or identifiable from the material it supplies, the danger remains that if the information were to be made public, the originating government would likely recognize the information as material it supplied in confidence. Thereafter, it would be reluctant to entrust the handling of its information to the discretion of the United States.

(44) The type of classified information provided by foreign government intelligence components can be categorized as information that identifies a named foreign government and detailed information provided by that foreign government. Exemption 1 has been asserted to protect information identifying a named foreign government and detailed information provided by that government. The detailed information is being withheld to protect the relationship and cooperative endeavors between this foreign government and the FBI, which is at issue in the records responsive to this case.

(45) The cooperative exchange of intelligence information between the foreign governments and the FBI was, and continues to be, with the express understanding that the information will be kept classified and not released to the public. Disclosure of the withheld information would violate the FBI's promise of confidentiality. A breach could reasonably be expected to strain relations between the United States and the foreign governments, chill the free flow of vital information to the intelligence and law enforcement agencies, and cause serious damage to the national security and the war on transnational terrorism. This information, which is under the control of the United States Government, is properly classified at the "Secret" level and withheld pursuant to E.O. 13,526 § 1.4(b), and is exempt from disclosure pursuant to Exemption 1.

(b)(1)-1 Intelligence Activities, Sources and Methods

(46) E.O. 13,526 § 1.4(c) authorizes the classification of "intelligence activities (including covert action), intelligence sources or methods, and cryptology," in order to protect classified intelligence sources, methods, and activities utilized by the FBI for gathering intelligence data.

(47) An intelligence activity or method includes any intelligence action or technique utilized by the FBI against a targeted individual or organization that has been determined to be of national security interest. An intelligence method is used to indicate any procedure (human or non-human) utilized to obtain information concerning such individual or organization. An intelligence activity or method has two characteristics. First, the intelligence activity or method -- and information generated by it -- is needed by U. S. Intelligence/Counterintelligence agencies to carry out their missions. Second, confidentiality must be maintained with respect to the activity or method if the viability, productivity and usefulness of its information is to be preserved. Information was withheld pursuant to Exemption 1 to protect intelligence methods utilized by the FBI for gathering intelligence data.

(48) The classified material here would, if disclosed, reveal actual intelligence activities and methods used by the FBI against specific targets of foreign counterintelligence investigations or operations; identify a target of a foreign counterintelligence investigation; or disclose the intelligence-gathering capabilities of the activities or methods directed at specific targets. The information obtained from the intelligence activities or methods is very specific in nature, provided during a specific time period, and known to very few individuals.

(49) It is my determination that the disclosure of the specific information describing the intelligence activities or methods withheld in this case, which are still used by the FBI today to gather intelligence information, could reasonably be expected to cause serious damage to the national security for the following reasons: (a) disclosure would allow hostile entities to discover the current intelligence-gathering methods used; (b) disclosure would reveal current specific targets of FBI's national security investigations; and (c) disclosure would reveal the determination of criteria used and priorities assigned to current intelligence or counterintelligence investigations. With the aid of this detailed information, hostile entities could develop countermeasures that would, in turn, severely disrupt the FBI's intelligence-gathering capabilities. This severe disruption would also result in severe damage to the FBI's efforts to detect and apprehend violators of national security and criminal laws of the United States. This information is currently and properly classified at the "Secret" level, in accordance with E.O. 13,526 § 1.4(c), and is exempt from disclosure pursuant to Exemption 1, as well Exemption 3/National Security Act of 1947, 50 U.S.C. § 3024(i)(1), as explained *infra*.

(50) The FBI protected the following categories of information specific to intelligence activities and methods because disclosure reasonably could be expected to cause serious damage to the national security: (a) detailed intelligence activity information compiled regarding a specific individual or organization of national security interest; (b) file numbers; and (c) the character and/or title of a case. Below is a more detailed discussion of each of these categories.

Detailed Intelligence Activities[16]

[16] The FBI applied Exemption 1 to protect this type of information only within the categorically denied records within Part II.

(51) The classified information withheld within these documents contains detailed intelligence activity information gathered or compiled by the FBI on a specific individual or organization of national security interest. The disclosure of this information could reasonably be expected to cause serious damage to the national security, as it would: (a) reveal the actual intelligence activity or method utilized by the FBI against a specific target; (b) disclose the intelligence-gathering capabilities of the method; and (c) provide an assessment of the intelligence source penetration of a specific target during a specific period of time. This information is properly classified at the "Secret" level and withheld pursuant to E.O. 13,526 § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

File Numbers

(52) The classified information withheld includes FBI file numbers assigned to specific intelligence activities, including channelization and dissemination instructions. Their release would lead to exposure of the particular intelligence activities and methods at issue. Individual file numbers are assigned by FBIHQ and field offices and contain a geographical prefix or the originating office and case number, which includes the numerical characterization of the type of investigation followed by a chronological number assigned to a specific investigation/activity.

(53) The disclosure of an intelligence file number in the aggregate will enable a hostile analyst to attribute any information released from the documents containing such a file number to that particular file. A hostile analyst can identify the specific intelligence activity by supplying further missing pieces. Hence, a partial mosaic of the activity begins to appear as more information is identified with the file leading to the exposure of actual current activities or

methods. Disclosure of file numbers will allow a hostile analyst, or anyone not privileged to this information, to patch bits and pieces of information together until the actual use of the application of the source or method can be determined. The identification of these intelligence methods, which continue to furnish positive intelligence information to this day, will severely limit their utility. In addition, disclosure will inform the United States' enemies of the possible range of our intelligence capabilities, as well as the probable intelligence that the FBI has gathered, or can collect, concerning them. This knowledge provides potential or actual violators of the United States' national security laws a means of deflection or avoidance of lawful regulations. Disclosure will allow countermeasures to be implemented, making future operations more difficult, and compromise other ongoing/planned intelligence operations. Accordingly, the release of the file numbers can lead to the exposure of the actual intelligence activity or method utilized in FBI investigations, and can reasonably be expected to cause serious damage to national security. These file numbers are properly classified at the "Secret" level pursuant to E.O. 13,526 § 1.4(c), and therefore, are exempt from disclosure pursuant to Exemption 1.[17]

Character and/or Title of Case[18]

(54) The classified information withheld identifies the character and/or title of the case for a specific type of intelligence activity directed at a specific target of national security interest.

---

[17] The FBI applied Exemption 1 to protect this type of information on the following Bates pages within Part I: Todashev-13-14, 18-19, 25-26, 40-41, 44-45, 50, 72, 85, 139, 141-142, 144, 148, 150, 489, 818-820, 837-838, 842, 849, 962, 969, 974, 990. The FBI also applied Exemption 1 to protect this type of information in the records within Part II.

[18] The FBI applied Exemption 1 to protect this type of information only within the categorically denied records within Part II.

Disclosure of the characterization and/or title of the case could reasonably be expected to cause serious damage to the national security, as it would: (a) disclose a particular intelligence or counterintelligence investigation; (b) disclose the nature, scope or thrust of the investigation; and (c) reveal the manner of acquisition of the intelligence or counterintelligence information. This information is properly classified at the "Secret" level pursuant to E.O. 13,526 § 1.4(c) and therefore, is exempt from disclosure pursuant to Exemption 1.

E.O. 13,526 § 1.4(d) – Foreign Relations or Foreign Activities[19]

(55) E.O. 13,526 § 1.4 (d) authorizes the classification of information concerning foreign relations or foreign activities of the United States, including confidential sources. The classified information withheld here contains sensitive intelligence information gathered by the United States either about or from a foreign country. This information is sensitive due in part to the delicate nature of international diplomacy, and must be handled with care so as not to jeopardize the fragile relationships that exist between the United States and certain foreign governments.

(56) The unauthorized disclosure of information concerning foreign relations or foreign activities of the United States can reasonably be expected to lead to diplomatic or economic retaliation against the United States; identify the target, scope, or time frame of intelligence activities of the United States in or about a foreign country, which may result in the curtailment or cessation of these activities; enable hostile entities to assess United States

[19] The FBI applied Exemption 1 to protect this type of information on Bates page Todashev-150 within Part I. Although the coded exemption cited on that page is (b)(1)-1, E.O. 13,526 § 1.4 (d) provides further justification, and is also asserted to protect this information. In addition, this section of E.O. 13,516 is noted in the classification stamp on the face of the document. The FBI also applied Exemption 1 to protect this type of information in the records within Part II.

intelligence gathering activities in or about a foreign country and devise countermeasures against these activities; or compromise cooperative foreign sources, which may jeopardize their safety and curtail the flow of information from these sources. Thus, the information about foreign relations or foreign activities which are withheld by the FBI is properly classified at the "Secret" level and pursuant to E.O. 13,526 § 1.4 (d), and is therefore, exempt from disclosure pursuant to Exemption 1.

Defendant's Burden of Establishing Exemption 1 Claims

(57) The information withheld in this case pursuant to Exemption 1 was examined in light of the body of information available to me concerning the national defense and foreign relations of the United States. This information was not examined in isolation. Instead, each piece of information was evaluated with careful consideration given to the impact that disclosure of this information will have on other sensitive information contained elsewhere in the United States intelligence community's files. Equal consideration was given to the impact that other information either in the public domain or likely known or suspected by present or potential adversaries of the United States would have upon the information I examined.

(58) In those instances where, in my judgment, the disclosure of this information could reasonably be expected to cause damage or serious damage to the national security, and its withholding outweighed the benefit of disclosure, I exercised my prerogative as an original classification authority and designated that information as classified in the interest of national security at the "Secret" level, and invoked FOIA Exemption 1 to prevent disclosure. The explanations set forth below justifying the FBI's withholding of classified information were prepared with the intent that they be read with consideration given to the context in which the

classified information is found. This context includes not only the surrounding unclassified information, but also other information already in the public domain, as well as information likely known or suspected by hostile intelligence entities. It is my judgment that any greater specificity in the descriptions and justifications set forth with respect to information relating to foreign government relations or foreign activities and intelligence sources and methods of the United States could reasonably be expected to jeopardize the national security of the United States.

EXEMPTION 3 – INFORMATION PROTECTED BY STATUTE

(59) Exemption 3 exempts information when another federal statute prohibits its disclosure provided that either the statute "requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue," or the statute "establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3). Moreover, if the withholding statute was enacted after October 28, 2009 (the date of enactment of the OPEN FOIA Act of 2009), then it must specifically cite to § 552(b)(3).

(b)(3)-1 National Security Act of 1947, 50 U.S.C. § 3024 (i)(1)

(60) In Category (b)(3)-1, the FBI withheld information pursuant to Section 102A(i)(1) of the National Security Act of 1947 ("NSA"), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA"), 50 U.S.C. § 3024(i)(1), which provides that the Director of National Intelligence ("DNI") "shall protect from unauthorized disclosure intelligence sources and methods."[20] As relevant to U.S.C. § 552(b)(3)(B), the National Security Act of 1947

[20] Section 102A(i)(1) of the National Security Act was previously codified at 50 U.S.C. § 403(i)(1). As a result of the reorganization of Title 50 of the U.S. Code, Section 102A(i)(1) is now codified at 50 U.S.C. § 3024(i)(1).

was enacted before the date of enactment of the OPEN FOIA Act of 2009. On its face, this federal statute leaves no discretion to agencies about withholding from the public information about intelligence sources and methods. Thus, the protection afforded to intelligence sources and methods by 50 U.S.C. § 3024(i)(1) is absolute. *See* CIA v. Sims, 471 U.S. 159 (1985).

(61) In order to fulfill its obligation of protecting intelligence sources and methods, the DNI is authorized to establish and implement guidelines for the Intelligence Community ("IC") for the classification of information under applicable laws, Executive Orders, or other Presidential Directives, and for access to and dissemination of intelligence. 50 U.S.C. § 3024(i)(1). In implementing this authority, the DNI promulgated Intelligence Community Directive 700, which provides that IC elements shall protect "national intelligence and intelligence sources and methods and activities from unauthorized disclosure."[21] The FBI is one of 17 member agencies comprising the IC, and as such must protect intelligence sources and methods.

(62) Given the plain Congressional mandate to protect the IC's sources and methods of gathering intelligence, the FBI has determined that intelligence sources and methods would be revealed if any of the withheld information is disclosed to Plaintiff. Therefore, the FBI is prohibited from disclosing such information under § 3024 (i)(1).[22]

(63) The FBI is asserting Exemption 3 in this case, in conjunction with Exemption 1, to

---

[21] Intelligence Community Directive (ICD) 700, date June 7 2012, at ¶ 2a.

[22] Although § 3024 (i)(1) does not impose a requirement to articulate harm, disclosure of this information presents a bona fide opportunity for individuals to develop and implement countermeasures, resulting in the loss of significant intelligence information, sources, and methods relied upon by national policymakers and the IC to safeguard national security.

protect information relating to foreign government relations or foreign activities, and intelligence sources and methods of the United States. Additionally, the FBI asserted exemption 3 in conjunction with exemption 1 to protect classified file numbers and foreign relationships related to the National Foreign Intelligence Program ("NFIP"). The NFIP is now known as the National Intelligence Program ("NIP").[23] The NIP consists of all programs, projects, and activities of the Intelligence Community, as well as any other programs of the Intelligence Community designated jointly by the Director and the head of a United States department or agency or by the President.[24] The activities of the Intelligence Community include the strategic use of various sources to obtain intelligence related information and are conducted through a myriad of available methods of intelligence gathering, not all of which are known to the public. As a federal agency within the Intelligence Community and a federal law enforcement agency, some of the FBI's programs and/or activities relate to the NIP. With regard to the pages at issue here, the FBI protected file numbers and foreign relationships, methods, and activities related to the NIP classified at the "Secret" level pursuant to (b)(1)-1 and (b)(3)-1 (50 U.S.C. § 3024(i)(1)), because release would not only cause serious damage to national security, it would also reveal intelligence sources and methods requiring protection under the National Security Act of 1947. Notably, § 3024 (i)(1) protects sources and methods regardless of whether they are classified. *See* Sims, 471 U.S. at

---

[23] *See* Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA") Title 1, Subtitle G, Section 1074 of Public Law 108-458, where the National Foreign Intelligence Program was re-designated as the National Intelligence Program.

[24] *See* Executive Order 12333, paragraph 3.5(j).

176. Accordingly, the FBI has withheld this information pursuant to Exemption 3, in conjunction with § 3024 (i)(1).[25]

Additional Exemption 3 Sub-Categories Applicable Only to the Records Categorically Exempt Pursuant to (b)(7)(A) (Part II)

Federal Grand Jury information (Federal Rule of Criminal Procedure 6(e))

(64) Within the pending investigative files at issue, there exists information exempt from disclosure pursuant to FOIA Exemption (b)(3), as this information is protected under Federal Rule of Criminal Procedure 6(e). As relevant to 5 U.S.C. § 552(b)(3)(B), Rule 6(e) is a statute enacted before the date of enactment of the OPEN FOIA Act of 2009.[26] It is well established that Rule 6(e) embodies a broad, sweeping policy of preserving the secrecy of grand jury material regardless of the substance in which the material is contained. The records responsive to Plaintiff's requests reflect that one or more federal grand juries were empaneled in relation to the investigation(s) at issue here, and information in the investigative files responsive to Plaintiffs' requests reveals matters occurring before the grand jury/juries. Specifically, the investigative files contain information about the names of recipients of federal grand jury subpoenas; information that identifies specific records subpoenaed by a federal grand jury; and copies of specific records provided to a federal grand jury in response to federal grand jury

[25] The FBI asserted Exemption (b)(3)-1 on the following Bates pages within Part I: Todashev-13-14, 18-19, 25-26, 40-41, 44-45, 50, 72, 85, 139, 141-142, 144, 148, 150, 489, 818-820, 837-838, 842, 849, 962, 969, 974, 990. The FBI also asserted Exemption (b)(3)-1 to protect information in the records within Part II.

[26] The OPEN FOIA Act of 2009 was enacted October 28, 2009. *See* Pub.L. 111-83, 123 Stat. 2142, 2184.

subpoenas. Any disclosure of this information would clearly violate the secrecy of the grand jury proceedings and could reveal the inner workings of a federal grand jury. Accordingly, this information is exempt from disclosure pursuant to FOIA Exemption (b)(3), in conjunction with Rule 6(e).

Information Exempted by 31 U.S.C. § 5319 (Bank Secrecy Act – "BSA")

(65) The U.S. Department of the Treasury established the Financial Crimes Enforcement Network ("FinCEN") in 1990 to provide a government-wide multisource financial intelligence and analysis network. FinCEN's mission is to enhance U.S. national security, deter and detect criminal activity, and safeguard financial systems from abuse by promoting transparency in the U.S. and international financial systems. FinCEN has primary responsibility for implementation of the provisions of the Bank Secrecy Act ("BSA"), 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951-1959, and 31 U.S.C. §§ 5311-5332.[27] As relevant to 5 U.S.C. § 552 (b)(3)(B), the BSA is a statute enacted before the date of enactment of the OPEN FOIA Act of 2009.

(66) The BSA authorizes the Secretary of the Treasury, inter alia, to issue regulations requiring financial institutions to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory matters, and to implement anti-money laundering programs and compliance procedures. The BSA specifically provides that reports collected pursuant to the BSA, and records of those reports, are exempt from disclosure under the FOIA. See 31 U.S.C. § 5319.

(67) Hundreds of thousands of financial institutions are subject to the BSA reporting

[27] The BSA was enacted in 1970 (Pub. L. No. 91-508, 84 Stat 1114-2).

and record-keeping requirements. These include depository institutions (e.g., banks, credit unions and thrifts); brokers or dealers in securities; insurance companies that issue or underwrite certain products; money services businesses (e.g., money transmitters; issuers, redeemers and sellers of money orders and travelers' checks; check cashers and currency exchangers); casinos and card clubs; and dealers in precious metals, stones, or jewels. Reports filed pursuant to the BSA, and records of reports, are exempt from disclosure under the FOIA, 5 U.S.C. § 552. (See 31 U.S.C. § 5319).

(68) Within the pending investigative documents at issue there exists information obtained through the BSA during the course of criminal investigative activities. The FBI obtained this information from FinCEN. The BSA provision found at 31 U.S.C. § 5319 provides that "a [BSA] report and records of reports are exempt from disclosure under section 552 of title 5." Pursuant to this statutory authority, FinCEN promulgated a regulation, found at 31 C.F.R. § 103.54, which specifically exempts BSA records from FOIA disclosure. The FBI is statutorily prohibited from identifying anything regarding the particular information withheld in these records. Therefore, this information is exempt from disclosure pursuant to FOIA Exemption (b)(3).

Exemption 5 Categories Applicable Only to the Records Categorically Exempt Pursuant to (b)(7)(A) (Part II)

EXEMPTION (b)(5) – PRIVILEGED INFORMATION

(69) 5 U.S.C. § 552(b)(5) exempts from disclosure "inter-agency or intra-agency

memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." This exemption has been construed to exempt those documents or information normally privileged in the civil discovery context, including, as is the case within the pending investigative documents at issue, the Attorney-Client Privilege, the Attorney Work Product Privilege and the Deliberative Process Privilege.

Attorney-Client Privileged Information

(70) The FBI asserts the Attorney-Client Privilege to protect confidential communications between FBI employees (clients) seeking legal advice from agency attorneys (professional legal advisers) in their capacities as lawyers, within the pending documents at issue. The Attorney-Client privilege encompasses confidential communications between these agency attorneys and FBI employees seeking legal advice. These communications between clients and attorneys were made in confidence, were not shared with or circulated to individuals outside the attorney-client relationship, and were made for the purpose of securing legal assistance or advice. Disclosure of these communications between the FBI attorneys and their clients would inhibit candor between the clients and their attorneys in relation to the issues about which they are seeking legal advice. Such candor and full disclosure is necessary in order to ensure that thorough and sound legal advice is provided. Such communications are permanently protected from disclosure by the legal adviser unless the client waives the protection. Accordingly, this information is exempt from disclosure pursuant to FOIA Exemption (b)(5).

Attorney Work Product Privileged Information

(71) Within the pending documents at issue, the FBI asserts the Attorney Work

Product Privilege to protect privileged attorney work products. The attorney work product privilege protects such tangible and intangible items as interviews, memoranda, correspondence, mental impressions, and personal beliefs prepared or developed by an attorney in anticipation of litigation. The privilege is predicated on the recognition that proper preparation of a case depends on an attorney's ability to assemble information, sort relevant from irrelevant facts, and prepare his/her legal theories and strategies without intrusive or needless scrutiny. The FBI is specifically asserting the Attorney Work Product Privilege to protect materials created by agency attorneys who were evaluating and annotating documents to be filed in court by FBI personnel. This information satisfies FOIA Exemption (b)(5)'s threshold because these records were exchanged between FBI Attorneys and FBI employees who were coordinating strategies of how to create the most effective/persuasive legal arguments in documents to be filed with Untied States courts. Furthermore, these records are quintessential attorney work products and readily satisfy the elements of the attorney work product privilege because they were created by attorneys during as part of the attorneys' representation of the government. Finally, because the Attorney Work Product Privilege protects both factual and deliberative material, segregation is not required. Accordingly, this information is exempt from disclosure pursuant to FOIA Exemption (b)(5).

Deliberative Process Privilege Information

(72) The FBI asserts Exemption (b)(5) to protect privileged deliberative materials. The deliberative process privilege protects the internal deliberations of the government by exempting from release recommendations, analyses, speculation and other non-factual information prepared

in anticipation of agency decision-making. The general purpose of the deliberative process privilege is to prevent injury to the quality of agency decisions. Thus, material containing or prepared in connection with the formulation of opinions, advice, evaluations, deliberations, policy formulation, proposals, conclusions or recommendations may properly be withheld. Release of this type of information would have an inhibitive effect upon the development of policy and administrative direction of an agency because it would chill the full and frank discussion between agency personnel regarding a decision. If agency personnel knew that their preliminary opinions, evaluations and comments would be released for public consumption, they may be more circumspect in what they put in writing, and thereby, impede a candid discussion of the issues surrounding a decision. Accordingly, this information is exempt from disclosure pursuant to FOIA Exemption (b)(5).

EXEMPTION 7 THRESHOLD

(73) Before an agency can invoke any of the harms enumerated in FOIA Exemption (b)(7), it must first demonstrate that the records or information at issue were compiled for law enforcement purposes. Pursuant to 28 U.S.C. §§ 533 and 534, and Executive Order 12,333 as implemented by the Attorney General's Guidelines for Domestic FBI Operations and 28 C.F.R. § 0.85, the FBI is the primary investigative agency of the federal government with authority and responsibility to investigate all violations of federal law not exclusively assigned to another agency, to conduct investigations and activities to protect the United States and its people from terrorism and threats to national security, and further the foreign intelligence objectives of the United States. Under this investigative authority, the FBI created the responsive pending

investigative records in this case as part/in furtherance of international terrorism investigations of Ibragim Todashev and others for engaging in criminal activities related to the Boston Marathon Bombing and other international terrorism activities.

(74) Thus, these records were compiled for a law enforcement purpose and they squarely fall within the law enforcement duties of the FBI. Therefore, the information readily meets the threshold requirement of Exemption 7.

EXEMPTIONS 6 AND 7(C) –INVASIONS OF PERSONAL PRIVACY

(75) Exemption 6 exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). All information that applies to a particular person falls within the scope of Exemption 6.

(76) Exemption 7(C) similarly exempts from disclosure "records or information compiled for law enforcement purposes [when disclosure] could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C).[28]

(77) When withholding information pursuant to these two exemptions, the FBI is required to balance the privacy interests of the individuals mentioned in these records against any

[28] The practice of the FBI is to assert Exemption 6 in conjunction with Exemption 7(C). Although the balancing test for Exemption 6 uses a "would constitute a clearly unwarranted invasion of personal privacy" standard and the test for Exemption 7(C) uses the lower standard of "could reasonably be expected to constitute an unwarranted invasion of personal privacy," the analysis and balancing required by both exemptions is sufficiently similar to warrant a consolidated discussion. The privacy interests are balanced against the public's interest in disclosure under both exemptions.

public interest in disclosure. In asserting these exemptions, each piece of information was scrutinized to determine the nature and strength of the privacy interest of every individual whose name and/or identifying information appears in the documents at issue. When withholding the information, the individual's privacy interest was balanced against the public's interest in disclosure. For purposes of these exemptions, a public interest exists only when information about an individual would shed light on the FBI's performance of its mission to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. In each instance where information was withheld pursuant to Exemptions 6 and 7(C), the FBI determined that the individuals' privacy interests outweighed any public interest in disclosure.

(b)(6)-1 and (b)(7)(C)-1 Names of FBI Special Agents / Support Personnel

(78) In Category (b)(6)-1 and (b)(7)(C)-1, the FBI protected the names and identifying information[29] of FBI Special Agents ("SAs") and support personnel who were responsible for conducting, supervising, and/or maintaining the investigative activities reflected in the documents responsive to Plaintiff's FOIA request. These responsibilities included conducting interviews and compiling information, as well as reporting on the status of the investigations. Assignments of SAs to any particular investigation are not by choice. Publicity (adverse or otherwise) regarding any particular investigation to which they have been assigned may seriously prejudice

[29] As used in this declaration, the term "identifying information" includes, but is not limited to dates of birth, social security numbers, addresses, addresses, telephone numbers, and/or other personal information.

their effectiveness in conducting other investigations. The privacy consideration is also to protect FBI SAs, as individuals, from unnecessary, unofficial questioning as to the conduct of this or other investigations, whether or not they are currently employed by the FBI. FBI SAs conduct official inquiries into various criminal and national security violation cases. They come into contact with all strata of society, conducting searches and making arrests, both of which result in reasonable but nonetheless serious disturbances to people and their lives. It is possible for an individual targeted by such law enforcement actions to carry a grudge which may last for years. These individuals may seek revenge on the agents and other federal employees involved in a particular investigation. The publicity associated with the release of an agent's identity in connection with a particular investigation could trigger hostility toward a particular agent. Thus, SAs maintain substantial privacy interests in information about them in criminal investigative files. In contrast, there is no public interest to be served by disclosing the identities of the SAs to the public because their identities would not, themselves, significantly increase the public's understanding of the FBI's operations and activities. Accordingly, after balancing these SAs' substantial privacy interests against the non-existent public interest, the FBI properly protected the names of SAs pursuant to Exemptions 6 and 7(C).

(79) The names of FBI support employees were also protected. Support personnel are assigned to handle tasks related to the official investigations reflected in the documents responsive to Plaintiff's FOIA request. They were, and possibly are, in position of access to information regarding official law enforcement investigations, and therefore could become targets of harassing inquiries for unauthorized access to investigations if their identities were released.

The documents contain the names of FBI SAs and support personnel. The FBI balanced the SA's and support personnel's privacy interests against the public interest in disclosure and determined the release would not significantly increase the public's understanding of FBI operations and activities. Disclosure of the information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy. Thus, these individuals maintain substantial privacy interests in not having their identities disclosed. Accordingly, after balancing these employees' substantial privacy interests against the non-existent public interest, the FBI properly protected the names and identifying information of SAs and support personnel pursuant to FOIA Exemptions (b)(6)-1 and (b)(7)(C)-1.[30]

(b)(6)-2 and (b)(7)(C)-2 Names and/or Identifying Information of Local Law Enforcement Personnel

(80) In Category (b)(6)-2 and (b)(7)(C)-2, the FBI withheld the names and identifying information of local law enforcement personnel. These employees were acting in their official capacity and aided the FBI in the law enforcement investigative records responsive to Plaintiff's request. The rationale for protecting the identities of FBI SAs and support personnel discussed at paragraphs 78-79, *supra*, also supports withholding the names and identifying information of these local law enforcement personnel. To release the identities of these law enforcement

[30] The FBI asserted Exemptions (b)(6)-1 and (b)(7)(C)-1 on the following Bates pages within Part I: Todashev-2, 4-13, 15-16, 18, 20-21, 23-25, 27-33, 36-40, 42-44, 46-47, 49-52, 69-81, 83, 85-90, 92-106, 109-111, 113-118, 136, 138-145, 148-155, 163, 165-166, 168-180, 182, 184-185, 187, 189-191, 193, 201, 206-218, 251, 258, 489, 817-820, 822-834, 836-837, 839, 850-852, 854-864, 866-867, 870-878, 881-928, 932-935, 948-958, 962, 968-969, 972-973, 976-978, 980-981, 983-984, 986-992, 997, 1011, 1019-1020, 1022-1023, 1045, 1047-1055, 1058, 1086. The FBI also asserted Exemptions (b)(6)-1 and (b)(7)(C)-1 to protect information in the records within Part II..

personnel could subject them as individuals to unnecessary, unwarranted harassment which would constitute an unwarranted invasion of privacy. Furthermore, these individuals could become a prime target for compromise if their identities were known. There is no public interest to be served in releasing the identities of these individuals. The FBI concluded that the disclosure of this information would constitute a clearly unwarranted and an unwarranted invasion of their personal privacy. The FBI has properly withheld this information pursuant to FOIA Exemptions (b)(6)-2 and (b)(7)(C)-2.[31]

(b)(6)-3 and (b)(7)(C)-3 Names and/or Identifying Data of Third Parties of Investigative Interest

(81) In Category (b)(6)-3 and (b)(7)(C)-3, the FBI protected the names and identifying information of third party individuals who were of investigative interest to the FBI. Being linked with any law enforcement investigation carries a strong negative connotation and a stigma. To release the identities of these individuals to the public in this context could subject them to harassment or embarrassment, as well as undue public attention, whether or not they ever actually committed a crime. Accordingly, the FBI has determined these individuals maintain a substantial privacy interest in not having their identities disclosed. In making a determination whether to release the names and/or personal information concerning these third parties, the public's interest in disclosure was balanced against the individuals' right to privacy. The FBI

[31] The FBI asserted Exemptions (b)(6)-2 and (b)(7)(C)-2 on the following Bates pages within Part I: Todashev-24-26, 43, 49-52, 74, 103, 113, 118, 138-140, 850-858, 860-861, 863-864, 866-867, 871, 874-875, 881-888, 890-904, 906-920, 922-923, 925, 927, 935, 939-940, 942, 981, 986, 995-996, 999-1000, 1003-1004, 1007-1009, 1012-1019, 1045, 1054, 1071, 1076, 1082, 1085-1086. The FBI also asserted Exemptions (b)(6)-2 and (b)(7)(C)-2 to protect information in the records within Part II.

determined this information would not enlighten the public on how it conducts its internal operations and investigations. Accordingly, the FBI concluded the disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy. The FBI properly protected the names and identifying information of third parties of investigative interest pursuant to Exemptions (b)(6)-3 and (b)(7)(C)-3.[32]

(b)(6)-4 and (b)(7)(C)-4 Names of Non-FBI Federal Government Personnel and Foreign Law Enforcement or Intelligence Agency Personnel

(82) In Category (b)(6)-4 and (b)(7)(C)-4, the FBI protected the names and identifying information of non-FBI federal government personnel mentioned in records responsive to Plaintiff's request. Specifically, the FBI protected the names of Department of Justice personnel and foreign law enforcement or intelligence agency personnel. The relevant inquiry here is whether public access to this information would violate a viable privacy interest of these individuals, and whether there is a public interest in releasing their identities. Disclosure of these individuals' identities and identifying information could subject these personnel to unauthorized inquiries and harassment and would constitute a clearly unwarranted invasion of their personal privacy. The rationale for protecting non-FBI federal employees is the same as that for FBI

[32] The FBI asserted Exemptions (b)(6)-3 and (b)(7)(C)-3 on the following Bates pages within Part I: Todashev-1-2, 5, 16, 19, 25-26, 29, 33-35, 38-39, 76-77, 81, 83-84, 88, 113, 139-140, 155, 163, 165-166, 168-182, 184-186, 189, 191, 193-195, 261-276, 278-279, 286, 289-290, 293-294, 297-299, 301-307, 311-314, 316-489, 492-497, 499-529, 533, 535-540, 546, 553, 560-563, 568-582, 585-588, 594, 596-602, 611-612, 623, 627, 631, 634-635, 646-647, 655-663, 666-671, 677-681, 684-687, 691-701, 707, 736-739, 765-766, 792-793, 797, 803-804, 806-807, 811-814, 816-820, 822, 836-837, 844-845, 847-849, 851, 853-855, 866, 874, 881, 886, 890, 897-899, 903, 905-906, 910-911, 914-915, 919-921, 923, 925, 928, 935-942, 948-949, 951-956, 996, 1019-1021, 1045, 1047, 1050, 1054-1055, 1058. The FBI also asserted Exemptions (b)(6)-3 and (b)(7)(C)-3 to protect information in the records within Part II.

employees discussed *supra*.

(83) In balancing the legitimate privacy interest of these individuals against any public interest in disclosure, the FBI determined that there is a complete lack of bona fide public interest in this information because its disclosure will not shed light on the operations and activities of the federal government. Accordingly, the FBI has concluded that the disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of these individuals' personal privacy. The FBI properly protected the names and identifying information of non-FBI federal government personnel pursuant to FOIA Exemptions (b)(6)-4 and (b)(7)(C)-4.[33]

(b)(6)-5 and (b)(7)(C)-5 Names and/or Identifying Information of Third Parties Merely Mentioned

(84) In Category (b)(6)-5 and (b)(7)(C)-5, the FBI protected the names and identifying information of third-parties who were merely mentioned in the responsive documents. The FBI has information about these third-parties in its files because these individuals were related either directly or indirectly with the investigation into the shooting death of Ibragim Todashev and the other pending investigations in the records at issue here. These individuals were not of investigative interest to the FBI. Despite the age of the documents, these third-parties maintain substantial and legitimate privacy interests in avoiding disclosure of this information and thereby being connected with a criminal investigation. Disclosure of these third-parties' names and/or identifying information in connection with an FBI investigation carries an extremely negative

[33] The FBI asserted Exemptions (b)(6)-4 and (b)(7)(C)-4 on the following Bates pages within Part I: Todashev-860, 864, 927, 1055, 1057-1059, 2045. The FBI also asserted Exemptions (b)(6)-4 and (b)(7)(C)-4 to protect information in the records within Part II.

connotation. Disclosure of their identities would subject these individuals to possible harassment or criticism and focus derogatory inferences and suspicion on them. The FBI also considered whether there was any public interest that would override these privacy interests, and concluded that disclosing information about individuals merely mentioned in an FBI file would not significantly increase the public's understanding of the operations and activities of the FBI. Accordingly, the FBI properly protected these individuals' privacy interests pursuant to FOIA Exemptions (b)(6)-5 and (b)(7)(C)-5.[34]

Additional Exemptions 6 & 7(C) Sub-Categories Applicable Only to the Records Categorically Exempt Pursuant to (b)(7)(A) (Part II)

Names and/or Identifying Information of Third Parties Who Provided Information to the FBI

(85) FOIA Exemptions (b)(6) and (b)(7)(C) for this category have only been asserted in this category to protect the names and identifying information of individuals who were interviewed by the FBI (and subsequently provided information) during the course of the investigations described in the records categorically exempt pursuant to (b)(7)(A). The FBI has found that information provided by individuals during an interview is one of the most productive investigative tools used by law enforcement agencies. The largest roadblock to successfully obtaining the desired information through an interview is fear by the interviewee that his/her identity will possibly be exposed and consequently that he/she could be harassed, intimidated, or

[34] The FBI asserted Exemptions (b)(6)-5 and (b)(7)(C)-5 on the following Bates pages within Part I: Todashev-13-14, 33-35, 38, 51, 83, 105-108, 181, 839, 842-843, 851-852, 861, 866, 928-930, 935-941, 993-995, 998-999, 1001-1003, 1005-1010, 1012-1017, 1021, 1055-1056, 1058-1059, 1077-1081. The FBI also asserted Exemptions (b)(6)-5 and (b)(7)(C)-5 to protect information in the records within Part II.

threatened with legal or economic reprisal, or possible physical harm. To surmount these obstacles, persons interviewed by the FBI must be assured that their names and personal identifying information will be held in the strictest confidence. Thus, the FBI has determined that the third party interviewees maintain substantial privacy interests in not having their identities disclosed. In contrast, the FBI could not identify any public interest in the disclosure of this information because the disclosure of these third parties' names and identifying information would not shed light on the operations and activities of the FBI. Accordingly, the FBI concluded that the disclosure of this information would unwarrantedly invade these individuals' personal privacy interests; therefore, this information is exempt from disclosure pursuant to FOIA Exemptions (b)(6) and (b)(7)(C).

EXEMPTION 7(A)—PENDING LAW ENFORCEMENT PROCEEDINGS[35]

(86) Exemption (b)(7)(A) protects records or information compiled for law enforcement purposes when disclosure "could reasonably be expected to interfere with enforcement proceedings." 5 U.S.C. § 552(b)(7)(A).

(87) Application of Exemption (b)(7)(A) requires: the existence of law enforcement records; a pending prospective law enforcement proceeding; and a reasonable expectation that release would interfere with the enforcement proceeding.

(b)(7)(A)-1 Information That Could Reasonably be Expected to Interfere with Pending Enforcement Proceedings

[35] This (b)(7)(A) explanation here justifies the FBI's limited assertion of the Exemption within the records encompassed in Part I. The FBI's explanation for categorically applying this Exemption to the records in Part II is explained in detail *infra* at ¶¶ 134-142.

(88) In the records within Part I, the FBI protected file numbers and other information directly related to pending investigations on the following Bates pages: Todashev-545-546, 846-847, 853-855, 867, 874, 885-886, 899, 905-906, 911, 914-915, 941-946.

(89) Release of the file numbers or other identifying information of on-going criminal and/or International Terrorism ("IT") investigations could not only result in the acknowledgement of the existence of a particular investigation but also in the identification of suspects, thus jeopardizing the investigation and prosecution of suspects. The records in the investigations have themselves been protected pursuant to FOIA Exemption (b)(7)(A); in order to prevent interference with the investigations.

Exemption 7(D) Sub-Categories Applicable Only to the Records Categorically Exempt Pursuant to (b)(7)(A) (Part II)

EXEMPTION (b)(7)(D) – CONFIDENTIAL SOURCE INFORMATION

(90) Exemption 7(D) protects "records or information compiled for law enforcement purposes [when disclosure] could reasonably be expected to disclose the identity of a confidential source, including a state, local or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source. 5 U.S.C. § 552(b)(7)(D).

(91) Numerous confidential sources report to the FBI on a regular basis and are "informants" within the common meaning of the term; these sources provide information under an express assurance of confidentiality. Still other individuals are interviewed under

circumstances from which an assurance of confidentiality can reasonably be inferred. These individuals are considered to be confidential sources because they furnished information only with the understanding that their identities and the information provided would not be released outside the FBI. Information provided by these individuals is singular in nature, and if released, could reveal their identity.

Names and/or Information Provided by Third Parties (Implied Confidentiality)

(92) Within the pending investigative files at issue, Exemption (b)(7)(D) has been applied to protect the names and identifying information of third parties, including individuals and commercial sources (corporate entities), that provided information to the FBI under implied assurances of confidentiality. The FBI also relied on Exemption (b)(7)(D) to protect the information provided by these sources. These sources provided specific detailed information that is singular in nature concerning the pending investigations at issue. The disclosure of the identities of these individuals and commercial entities could have disastrous consequences.

(93) These sources provided information of value to the FBI pertaining to possible criminal activities to include violent international terrorism, and in doing so, placed themselves in harm's way should the public become aware of their cooperation with the FBI. Specifically, within the responsive documents, the FBI inferred that individuals provided information to the FBI only because they believed their cooperation with, and the information they provided, would remain confidential. The FBI determined that based on these sources' closeness to those on whom they provided information, their social positions, and/or status within the business community, they face high risks for retaliation if their cooperation with the FBI was released in

this context. Potential forms of retaliation could include the following: embarrassment within communities where cooperation with law enforcement carries negative connotations; harassment by the media and those interested in the investigations at issue; ridicule by friends and/or family for informing on those close to the sources; intimidation by criminals wishing to dissuade people from cooperating with law enforcement; financial consequences for corporate entities and/or employees willing to share key information with law enforcement concerning their customers/employers/coworkers/employees; and/or physical harm by the violent international terrorists under investigation in the records at issue. Accordingly, it is reasonable in this case to infer that each of these sources provided information to the FBI under circumstances from which an assurance of confidentiality may be implied. The identities of those providing information and the information they provided warrants protections under Exemption FOIA Exemption (b)(7)(D). The preservation of the confidentiality of the identities of and information provided by sources is essential to effective law enforcement. Disclosure could have a disastrous impact upon the ability to obtain this kind of information in the future, and would have a chilling effect upon the free flow of information essential to pursue and resolve criminal investigations. Thus, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(D).

Information Provided by Foreign Law Enforcement/Intelligence Authorities (Express Confidentiality)

(94) FOIA Exemption (b)(7)(D) has been asserted to protect the identities of and information provided to the FBI by foreign law enforcement/intelligence authorities. The confidentiality of these foreign law enforcement/intelligence authorities is given under express assurances of confidentiality according to the Foreign Government Information Classification

Guide #1 (G-1 Guide) issued in accordance with E.O. 13,526, the Information Security Oversight Office (ISOO), the FBI Security Policy Manual, and the designated Original Classification Authority (OCA) of the Executive Assistance Director, National Security Branch. During the course of the FBI's intelligence investigations, it receives information from foreign government entities regarding on-going investigations. The FBI has many agreements with foreign governments under which security and/or criminal law enforcement information is exchanged. These agreements specify the extent of confidentiality requested by the respective foreign government entity. In this case, the FBI has express confidentiality agreements with the foreign governments and/or foreign law enforcement entities that provided information to the FBI during the conduct of intelligence investigations. The FBI's agreements with these foreign government entities provide express assurances that the FBI will not disclose their identities, the identities of their personnel, or the information that they provided to the FBI. If the FBI were to disclose the identities of these foreign government agencies, the names of their personnel, or the information they provided, such a disclosure would violate these agreements and have a chilling effect on the FBI's relationship with these entities. Furthermore, such a disclosure would also have a chilling effect on the FBI's relationships with other foreign law enforcement agencies that have entered into similar agreements with the FBI. Accordingly, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(D).

Information Provided by State or Local Law Enforcement Authorities (Implied Confidentiality)

(95) FOIA Exemption (b)(7)(D) has been asserted to protect the names, identifying information, and information provided to the FBI by state or local law enforcement authorities

under implied assurances of confidentiality. Certainly, the FBI does not infer that all state or local law enforcement authorities who cooperate in federal investigations do so with expectations of confidentiality. However, under some circumstances, such an expectation may be inferred. Here, law enforcement authorities provided specific detailed information of value to the FBI that is singular in nature concerning a specific investigation pertaining to possible criminal activities, including violent international terrorism. Specifically, within the responsive documents, the FBI inferred that state or local law enforcement authorities provided information to the FBI with an expectation that their involvement in the investigation, and/or the information they provided, would remain confidential because: (a) the information and assistance provided would disclose law enforcement techniques utilized by state/local law enforcement, and/or details about law enforcement techniques, that are not publicly known; and the information provided would reveal sources and methods of state/local law enforcement evidence collection. The disclosure of this information could have disastrous consequences. If this information were released to the public under FOIA, these state and local law enforcement authorities could decide not to provide assistance to the FBI in the future for fear that their non-public law enforcement techniques, and sources and methods of evidence collection would be publicly disclosed by the FBI. Additionally, the FBI's disclosure of such information could cause the state and local law enforcement authorities to come under heavy scrutiny by their potential information sources as they could be viewed as having had a hand in the disclosure of this type of confidential information. Accordingly, it is reasonable for the FBI to infer that these state and law enforcement authorities provided this information to the FBI with an implied assurance of

confidentiality. The preservation of the confidentiality of the identities of and information provided by state and local law enforcement authorities is essential to effective law enforcement. Disclosure could have a disastrous impact upon the FBI's ability to obtain this kind of information in the future, and would have a chilling effect upon the free flow of essential information from the FBI's state and local law enforcement partners. Thus, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(D).

Names, Identifying Information, and/or Information Provided by Third Parties (Express Confidentiality)

(96) FOIA Exemption (b)(7)(D) has been asserted to protect the names and identifying information of third parties that provided information to the FBI under express assurances of confidentiality, as indicated by symbol source numbers (described further *infra*) or other forms of express confidentiality agreements. The FBI also relied on Exemption 7(D) to protect the information provided by these sources. Information provided by these sources is one of the most productive investigative tools utilized by law enforcement agencies. The largest roadblock in successfully obtaining the desired information is fear of exposure. Such exposure could result in harassment, intimidation, legal or economic reprisal, or possible physical harm. In order to surmount these obstacles, sources providing information under express assurances of confidentiality must be able to rely on the FBI's guarantee that information received from them will be held in the strictest confidence.

(97) When protecting sources who provided information under express assurances of confidentiality, the FBI utilized Exemption (b)(7)(D) to protect the permanent source symbol numbers of FBI sources mentioned in the responsive pending documents. The FBI assigns

permanent source symbol numbers in sequential order to confidential informants who report information to the FBI on a regular basis pursuant to an express assurance of confidentiality. In this case, the FBI did not refer to the confidential source by his or her true name. Instead, the source was referred to only by his or her individually assigned permanent source symbol number. The FBI obtained information from this confidential source regarding activities of investigative interest in the investigative files responsive to Plaintiff's requests.

(98) If the FBI disclosed the confidential source symbol number of these informants, their identities could be ascertained by persons knowledgeable of the FBI's investigations discussed in the records at issue. Furthermore, if the FBI disclosed these sources' identities, the informants, as well as their families, could be subjected to embarrassment, humiliation, and/or physical or mental harm. Disclosure of a source symbol number at various times and in various documents could identify a confidential FBI source because such disclosure would reveal the connections of the confidential informant to the subject matter of these documents. Repeated release of the confidential source symbol number along with the information provided by the confidential source would narrow the possibilities of his or her true identity. This is especially true inasmuch as each confidential source symbol number is assigned to only one confidential informant.

(99) Additionally, in order to further protect sources who provided information to the FBI under express assurances of confidentiality, (b)(7)(D) is also being asserted to protect confidential informant file numbers of permanent confidential symbol number sources of the FBI. Similar in usage to the confidential source symbol numbers, these file numbers are also assigned

in sequential order to confidential informants who report information to the FBI on a regular basis pursuant to an express assurance of confidentiality. The confidential source file number is unique to the particular confidential informant and is used only in documentation relating to that particular informant.

(100) Disclosure of confidential informant file numbers at various times and in various documents could ultimately identify these sources because it would reveal the connections of confidential informants to the information provided by them. Repeated release of confidential source file numbers along with the information provided by these confidential informants would narrow the possibilities of their true identities. This is especially true because each confidential source file number is assigned to only one confidential informant.

(101) In summation, the FBI asserts FOIA Exemption (b)(7)(D) to protect personal identifiers (to include source symbol numbers and source file numbers) of sources who provided information to the FBI under express assurances of confidentiality, and any information provided by these sources.. The disclosure of the identities of these confidential sources would have a chilling effect on the activities and cooperation of both current and future FBI confidential informants. The FBI has found that it is only with the understanding of complete confidentiality that the assistance of such informants can be enlisted, and only through this assurance of confidentiality that these informants can be persuaded to continue their assistance in providing information to the FBI in the future. Disclosure would not serve any public interest and would impede the effectiveness of the FBI to employ similar sources to investigate and prevent crime in future investigations; therefore this information is exempt from disclosure pursuant to FOIA

Exemption (b)(7)(D).

EXEMPTION 7(E) – INVESTIGATIVE TECHNIQUES AND PROCEDURES

(102) Exemption 7(E) protects records and information compiled for law enforcement purposes that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552 (b)(7)(E).

(103) Exemption 7(E) has been asserted to protect information from these documents, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions, that could reasonably be expected to risk circumvention of the law. This exemption affords categorical protection to techniques and procedures used in law enforcement investigations; it protects techniques and procedures that are not well-known to the public as well as non-public details about the use of well-known techniques and procedures.

(b)(7)(E)-2 FBI Internal Non-Public Intranet Web Addresses

(104) In Category (b)(7)(E)-2, the FBI protected internal non-public Intranet web addresses specific to the FBI. Release of this type of information would provide criminals with potential targets for cyber attack. With this knowledge, criminals or adversaries with cyber capabilities could exploit the FBI's Information Technology system to gain unauthorized access to, view and manipulate data on, or otherwise interfere with the FBI's unclassified, but non-public Intranet protocol. In addition, such exploitation or access could arm individuals with further

information or ability to circumvent the law and allow individuals to disrupt official FBI business. Thus, the FBI properly protected this information from disclosure pursuant to FOIA Exemption 7(E).[36]

(b)(7)(E)-3 Sensitive FBI Squads and/or Units

(105) The FBI applied Category (b)(7)(E)-3 to protect the names, numbers, alpha designators, and other descriptive information pertaining to certain sensitive FBI squads and units. The existence of these units and their specific law enforcement/intelligence gathering missions have not been publicly released. Many of these sensitive squads/units have been assigned to investigate highly specific types of crime or perform other highly specific law enforcement functions. The protected information includes lists of services provided by these units, in addition to other descriptive information. Releasing this information, within the context of the documents, would reveal the level of focus the FBI has applied to certain law enforcement functions. Providing criminals with the level of focus the FBI is applying to certain investigations and functions, particularly in a specific investigation, would allow those criminals to know where the FBI is focusing its limited resources. Terrorists or other criminals could then plan and structure their activities in a manner that which avoids the FBI's strengths and exploits its weaknesses, making it easier for them to circumvent the law.

(106) Additionally, within the documents that are categorically exempt pursuant to Exemption 7A (Part II), there exist descriptions of the size and lists of participants in particular

[36] The FBI asserted Exemption (b)(7)(E)-2 on the following Bates pages within Part I: Todashev-824-828, 876, 996. The FBI also asserted Exemption (b)(7)(E)-2 to protect information in the records within Part II.

FBI Units/Task Forces. As these Units/Task Forces have been assembled to pursue specific investigative goals, revealing this type of information would reveal the very scope of the methods, techniques, and/or capabilities of the Units/Task Forces. Providing criminals with the level of focus the FBI is applying to these types of techniques/methods/capabilities would provide criminals with an idea as to where the FBI is focusing its limited resources. It would also reveal in which regions of the United States these crimes/national security threats are receiving the most focus by the FBI. Criminals could then plan and structure their activities to that avoid the FBI's investigative strengths, exploit its weaknesses, and circumvent the law.

(107) Additionally, many of these Units/Squads exist specifically to implement certain law enforcement/intelligence gathering techniques available to the FBI. Releasing information concerning these squads would thus reveal the nature of the FBI's use and/or reliance on these law enforcement/intelligence gathering techniques. Revealing this information within the context of these documents would allow criminals to judge which techniques are most likely to be used by the FBI in certain investigative situations. These criminals could then structure their behavior to avoid detection and disruption by the FBI, via these very techniques.

(108) In summation, revealing the nature and existence of these sensitive investigative squads/units would enable criminals to circumvent the law by knowing the focus and the sensitive functions performed by these units, exploiting areas in which the FBI's resources are more limited, and avoiding specific law enforcement/intelligence gathering techniques where the FBI's focus is higher; therefore, this information exempt from disclosure pursuant to FOIA Exemption

(b)(7)(E).[37]

(b)(7)(E)-5 Sensitive FBI File Numbers and Descriptions

(109) Exemption (b)(7)(E)-5 has been asserted to protect sensitive FBI file numbers and descriptions of the sensitive investigations to which these files pertain. The name or nature of these files indicates which techniques and/or investigative strategies were utilized by the FBI in particular IT investigations. The FBI has determined that this exemption is appropriate for protecting these file numbers. FBI file numbers are created solely because of FBI investigations and as such the FBI has asserted protection for file numbers related to other sensitive criminal and/or national security investigations because those numbers exist solely because of the FBI's exercise of its law enforcement functions. Additionally, the release of file numbering convention identifies the investigative interest or priority given to such matters. Applying a mosaic analysis, suspects could use these numbers (indicative of investigative priority), in conjunction with other information known about other individuals and/or techniques, to change their pattern of activity to avoid detection, apprehension, or create alibis for suspected activities, etc. It is the assemblage of file numbers that risks harm if disclosed, not generally a single classification code in total isolation. This accumulation of file numbers is the crux of the "sensitive" term used here to describe the withheld file numbers or sub file names. The word "sensitive" in this context speaks to not only the potential harm to investigative focuses for future investigations categorized under these classification codes or the types of investigation which are taking or have already taken

[37] The FBI asserted Category (b)(7)(E)-3 on the following Bates pages within Part I: Todashev-88-89, 93-94, 96, 98, 115. The FBI also asserted Exemption (b)(7)(E)-3 to protect information in the records within Part II.

place, but also the circumvention of the law. To determine the sensitivity of certain file numbers, the FBI conducts a case-by-case analysis when determining whether to release a file number. Many factors go into this analysis such as the type or program under which the file number falls, whether the file is pending or closed, the subject or focus of the file, whether a file number has been previously released, and its interrelatedness with other criminal and/or national security investigations. These contextual factors become a type of litmus test to determine on a case-by-case basis if a file number can be released without harm or must be redacted. In instances where the FBI protected file numbers from disclosure, the FBI determined that release would provide key information to criminals that would risk circumvention of the FBI's law enforcement efforts; therefore, this information has been protected pursuant to FOIA Exemption 7(E)-5.[38] Additionally, in several instances, the FBI found that release of file numbers would also risk revealing classified/unclassified but sensitive intelligence sources and methods. In these instances, the FBI applied Exemption (b)(7)(E)-5 in conjunction with Exemptions (b)(1) and/or (b)(3).

(b)(7)(E)-6 Collection / Analysis of Information

(110) In Category (b)(7)(E)-6, the FBI protected methods that the FBI uses to collect and analyze the information that it obtains for investigative purposes. The release of this information would disclose the identity of methods used in the collection and analysis of information, including how and from where the FBI collects information and the methodologies

[38] The FBI asserted Exemption (b)(7)(E)-5 on Bates pages Todashev-876 and 990 within Part I. The FBI also asserted Exemption (b)(7)(E)-5 to protect information in the records within Part II.

employed to analyze it once collected. Such disclosures would enable subjects of FBI investigations to circumvent similar currently used techniques. The relative utility of these techniques could be diminished if the actual techniques were released in this matter. This in turn would facilitate the accumulation of information by investigative subjects regarding the circumstances under which the specific techniques were used or requested and the usefulness of the information obtained. Release of this type of information would enable criminals to educate themselves about the techniques employed for the collection and analysis of information and therefore allow these individuals to take countermeasures to circumvent the effectiveness of these techniques and to continue to violate the law and engage in intelligence, terrorist, and criminal activities. The FBI has properly withheld this information pursuant to FOIA Exemption (b)(7)(E)-6.[39]

(b)(7)(E)-7 Operational Directives

(111) Exemption 7(E) has been asserted to protect certain information contained in an Operational Order responsive to Plaintiff's request. This law enforcement material comprises operational directives that provide information and instruct FBI employees on the proper use of certain sensitive non-public FBI procedures, techniques, and guidance for conducting investigations. In the course of providing these instructions, these guides identify the procedures, techniques, and strategies at issue. Specifically, the protected information falls within both

[39] The FBI asserted Exemption (b)(7)(E)-6 on the following Bates pages within Part I: Todashev-12, 15, 21, 23, 29, 39, 42, 79, 83-84, 169, 196-200, 814, 816, 834-835, 974-975, 978-979, 982, 985, 987. The FBI also asserted Exemption (b)(7)(E)-6 to protect information in the records within Part II.

subtypes of 7(E): tactical information contained in operational plans and operational directives concerning sensitive investigative techniques and strategies. Releasing such information would not only provide sensitive, unknown investigative techniques, it would also reveal sensitive unknown uses of these specific techniques and procedures. If released, the information would provide individuals and entities with a unique look inside the FBI's law enforcement "playbooks." Armed with such information, criminals could predict how and when the FBI will respond to certain suspicious/criminal activities, and the investigative techniques the FBI is most likely to employ in those situations. This would afford criminals the ability to preemptively modify their behavior in a manner that avoids detection and disrupt the very investigative procedures, techniques, and strategies that this FBI guide is intended to protect. Consequently, the release of this information would increase the risk that targets of criminal investigations could develop countermeasures and avoid detection by interfering with the FBI's ability to effectively use these important law enforcement techniques. Release of this information would allow individuals and entities seeking to commit crimes an opportunity to avoid detection and circumvent the law. Accordingly, the FBI has properly withheld this information pursuant to FOIA Exemption (b)(7)(E)-7.[40]

Additional Underlying Exemption 7(E) Sub-Categories Applicable Only to the Records Categorically Exempt Pursuant to (b)(7)(A) (Part II)

Types and Timing of FBI Investigations

(112) Within the pending investigative documents at issue, there exists information

[40] The FBI asserted Exemption (b)(7)(E)-7 on the following Bates pages within Part I: Todashev-865-866, 868-870.

concerning the types of International Terrorism ("IT") investigations being pursued by the FBI on certain subjects, and the dates associated with these investigations. Information concerning the type and timing of particular investigations would provide criminals with a road map of how the FBI's investigations were progressing on certain subjects. This information would also give terrorists valuable insight into how the FBI develops its investigations on particular IT subjects and whether or when the FBI may act on the information it has gathered. Because release of this information would consequently make it easier for terrorists to time and structure their illegal activities accordingly in order to circumvent the FBI's attempts to enforce the law, this information has been protected pursuant to FOIA Exemption (b)(7)(E).

Sensitive Intelligence Gathering Techniques

(113) Within the pending investigative documents at issue in this litigation, there exists information pertaining to sensitive law enforcement methods that the FBI uses to obtain and analyze valuable intelligence information in current and prospective criminal, counterintelligence, and national security investigations. Revealing the specific details of how these techniques are employed, in what situations they are most effective, the types of targets against which these techniques are employed, and the nature of the information that can be gleaned via the uses of these techniques would be extremely detrimental to the FBI's ability to effective utilize these techniques. Release of this information would allow criminals and those who threaten the national security of the United States the ability to develop countermeasure to circumvent the ability of law enforcement officials to use this technique, rendering it useless to the FBI. This information is not publicly known. Disclosure would undoubtedly compromise a crucial means

of collecting intelligence information and severely hamper the FBI's law enforcement efforts to detect and apprehend individuals who seek to violate the United States' criminal and national security laws; therefore, this information has been withheld from disclosure pursuant to Exemption (b)(7)(E).

Administrative Burden/Limitations of Implementing Certain Law Enforcement/Intelligence Gathering Techniques

(114) Within the pending investigative documents, there exists information detailing the internal FBI limitations on specific law enforcement/intelligence gathering techniques. In order to ensure accountability and maintain the lawful integrity of its investigations, the FBI has created limits on when certain techniques and procedures can be employed and has established requirements for varying degrees of approval to ensure that the use of these techniques and procedures receives the appropriate level of oversight. This ensures that FBI employees utilize these techniques and procedures effectively, ethically, and within the parameters of federal law and DOJ guidelines. Adversely, these checks on the FBI's activities create an administrative burden which may slow and limit the FBI's response in certain investigative situations.

(115) These internal investigative limitations have not been released to the public. Disclosure of this information could increase the risk of circumvention of FBI investigative techniques or of substantive law. A person either considering committing a crime or attempting to evade detection, knowing that certain investigative activities are or are not prohibited during certain types of investigations and/or knowing that there are certain approvals needed prior to FBI action, can combine this knowledge with other information to determine whether his or her activities are likely to be detected. Similarly, knowledge that a particular activity will not be

approved absent certain types of information could be exploited by someone seeking to evade detection. Detailing the internal administrative burden of implementing certain techniques and the situations in which they are available to the FBI would allow criminals to preemptively predict how the FBI will attempt to detect and or disrupt their criminal activities. As release of this information would enable criminals to circumvent the law, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Definitions of Different Types of FBI Investigations

(116) Within the pending investigative documents at issue, there are numerous definitions concerning different types of sensitive FBI investigations. These definitions are strictly internal and have not been released to the public. The FBI has created specific criteria which FBI employees use to determine how investigations are categorized. As discussed previously in paragraph 114-115, *supra,* internal FBI policies establish that only certain types of investigative techniques are authorized for use within certain investigative categories. Thus, revealing how the investigations are defined by FBI personnel would reveal the investigative "toolbox" available to the FBI in certain situations. Releasing these investigation definitions would allow criminals to predict the FBI's responses and investigative strategies when pursuing certain types of criminal behavior/national security threats. Such a release would enable criminals to stay one step ahead of FBI investigators and enable them to circumvent the law; therefore, these investigation definitions are exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Unknown Investigative Targets

(117) Within the pending investigative documents at issue, there exists information concerning current targets of FBI investigative efforts. The FBI's investigative focus on these matters has been publicly disclosed. Revealing that these individuals and/or groups have been targeted by FBI investigations would alert these individuals and/or groups as to the FBI's investigative intentions. Provided with this information, these groups and individuals could take active measures to hinder the FBI's ability to investigate and collect evidence.

(118) Additionally, revealing why the FBI has targeted these individuals/groups for further investigation, within the context of these documents, would reveal key FBI targeting strategies. Criminals could use this information to judge what types of information/evidence triggers further interest by the FBI. This would allow criminals to effectively alter their behavior to avoid detection and/or further investigation by law enforcement.

(119) As releasing the targets of FBI investigative efforts would alert these targets to FBI investigative interest and reveal key FBI investigative targeting strategies, enabling criminals to deprive the FBI of key evidence and circumvent the law, this information is exempt pursuant to FOIA Exemption (b)(7)(E).

Computer Analysis Response Team ("CART") Data & Techniques

(120) The pending documents at issue contain numerous descriptions of FBI and local law enforcement computer and telephone analysis techniques utilized to gather evidence and draw conclusions within FBI investigations. In his October 16, 2014 speech at the Brooking Institution, FBI Director James Comey stated that "technology has forever changed the world we live in… Our phones and computers have become reflections of our personalities, our interests,

and our identities." Criminals, like most people, utilize their phones, computers, and digital media of other types to conduct their daily affairs, including their criminal activities. Law enforcement/intelligence gathering efforts often hinge on law enforcement agencies' abilities to analyze and interpret digital information. Law enforcement agencies must successfully examine digital evidence stored on desktop and laptop computers, CDs/DVDs, cell phones, digital cameras, digital media players, flash media, etc., in order to gather pertinent digital evidence.

(121) To accomplish the key task of exploiting digital evidence, law enforcement agencies have developed specific, targeted techniques to extract and interpret this data in a manner which may be later presented as evidence in law enforcement proceedings, or utilized to further intelligence gathering efforts. Providing detailed information concerning the software, equipment, techniques, procedures utilized and/or types of reports generated by these computer forensic examiners would impede the FBI's and its law enforcement partners' effectiveness in investigating crimes where evidence can be found on computers, telephones, and other digital media. It would also aid in circumvention of the law by providing criminals with examples of how to adjust their behavior in order to avoid detection, develop and/or utilize technology less susceptible to law enforcement detection or scrutiny, and/or use or develop technology to counteract techniques used by computer forensic examiners. Accordingly, this information is exempt pursuant to FOIA Exemption (b)(7)(E).

Sensitive Physical Surveillance ("FISUR") Techniques

(122) The pending documents at issue contain numerous descriptions of sensitive FBI FISUR techniques. These techniques and how they are utilized by the FBI have not been

revealed publicly. These techniques are essential to FBI personnel's abilities to physically track and observe subjects of FBI investigations, unbeknownst to those being observed. Maintaining stealth is absolutely key to conducting effective FISUR. If the FBI's presence is detected during these observations, criminals will most likely abort/modify their activities. Revealing these techniques would provide criminals with key information on how the FBI may detect their criminal activities through FISUR. Armed with this information, criminals could detect FBI FISUR activities, employ countermeasures to avoid FBI observance of their criminal behaviors, and/or simply modify their behavior in situations where they are most likely to be observed. In this manner, releasing these specifics concerning sensitive FBI FISUR techniques would deprive the FBI of a key investigative tool and enable criminals to circumvent the law; therefore, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Sensitive Electronic Surveillance ("ELSUR") Techniques

(123) The pending documents at issue contain numerous descriptions of sensitive FBI ELSUR techniques. These techniques have not been revealed to the public. These descriptions detail what can be detected through these techniques, and when they are most likely to be deployed in FBI investigations. Like FISUR, maintaining stealth is absolutely key to conducting effective ELSUR. Revealing these techniques would provide criminals with key information on how the FBI may detect their criminal activities through ELSUR. Armed with this information, criminals could better detect FBI ELSUR activities, employ countermeasures to avoid FBI observance of their electronic communications, and/or simply cease/modify their electronic communications in situations where they are most likely to be observed. In this manner,

releasing these specifics concerning sensitive FBI ELSUR techniques would deprive the FBI of key investigative tools and enable criminals to circumvent the law; therefore, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Intelligence Gathering Strategies and Goals

(124) Within the pending investigative documents at issue, there exists information concerning sensitive FBI intelligence gathering strategies and goals. Releasing this information would reveal intelligence gathering methodology, how specific information is used by the FBI, and would identify areas of focus for intelligence collection. Such a release would provide criminals an idea as to what types of information they need to safeguard and what types of activities they should avoid in order to thwart FBI intelligence gathering efforts. As criminals could also utilize this information to modify their behavior in a manner which avoids detection by FBI intelligence gathering efforts and continue to circumvent the law, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Techniques for Recruiting Confidential Human Sources ("CHSs")

(125) The pending documents at issue contain specific strategies and techniques for recruiting CHSs. Providing this information would allow criminals to predict the FBI's CHS recruitment strategies and gain insight regarding whom among them they should intimidate, coerce, or even eliminate to prevent detection by the FBI's CHS program. It would also allow criminals to pose as potentially valuable CHSs and feed the FBI faulty intelligence aimed at redirecting the bureau away from their own criminal activities. As releasing these sensitive strategies and techniques for recruiting effective CHSs could undermine the law enforcement

purpose of the FBI's CHS program, enabling criminals to circumvent the law, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Confidential Funding Techniques and Strategies

(126) The pending documents at issue contain passages that identify and describe confidential funding techniques and strategies. In many circumstances, the FBI must operate covertly in order to conduct successful investigations and intelligence gathering efforts. Key to maintaining operational security during covert FBI investigations is the FBI's ability to fund its covert operations without revealing agency involvement. In order to fund these types of covert efforts, the FBI has developed specific techniques and strategies which enable the FBI to provide undercover assets with the money they need to pursue convert investigations without revealing their connection to law enforcement. Revealing these confidential funding techniques and strategies would allow criminals to detect the FBI's covert efforts by tracing FBI funds from the agency to its covert operations and operatives. This would allow criminals to determine whether or not they are under investigation by the FBI and allow them to pinpoint which of their associates were actually working for the FBI. This would enable these criminals to preemptively abort their criminal plots or take further measures to avoid detection and/or disruption by the FBI. Additionally, if criminals found that one of their associates was an FBI informant or an undercover FBI agent, they may avoid, intimidate, coerce, eliminate or alienate this individual in order to thwart the FBI's investigative efforts. As revealing the FBI's confidential funding methods and strategies would markedly decrease the effectiveness of covert FBI investigations and intelligence gathering efforts as well as enable criminals to circumvent the law, this

information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Money Allocated for Certain Investigative Techniques

(127) In a few pages of the pending documents at issue, there are listings of the amounts of money that was spent by the FBI to implement an investigative technique. The FBI has limited resources, and must strategically allocate those resources to the locales and on the investigative efforts its sees as most useful to its law enforcement and intelligence gathering missions. Revealing the dollar amount spent on this technique would subsequently reveal the importance of the information gathered via this technique. While relatively insignificant on its own, combined with other bits of information released to the public by the FBI, this information could become a piece of a much larger understanding of the FBI's priorities and investigative efforts. Providing this information would allow criminals to gauge how they should modify their behavior to avoid/exploit the most effective/ineffective FBI techniques. As releasing this information would increase criminals' understandings of the FBI's strengths and weaknesses and allow them to utilize this understanding to circumvent the law, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Sensitive Operational Law Enforcement Strategies

(128) Within the pending investigative files at issue, there exists sensitive operational law enforcement strategies utilized by the FBI when investigating and apprehending known or suspected criminals. These sensitive operational law enforcement strategies have been developed for the purpose of investigating/apprehending known or suspected criminals in the most efficient and safe manner. These sensitive operational law enforcement strategies are not

known to the public. Releasing this information would provide criminals with information they could use to predict the actions of law enforcement personnel and evade detection and/or apprehension by law enforcement. In this manner, releasing this information would also make the tasks of investigating and apprehending known or suspected criminals much more dangerous for law enforcement personnel. As releasing this information would enable criminals to evade efforts by law enforcement personnel to investigate their criminal activities and/or apprehend their persons, this information is exempt pursuant to FOIA Exemption (b)(7)(E).

Counter-Surveillance Techniques

(129) In a few pages of the pending documents at issue, there are descriptions of counter-surveillance techniques observed and described by FBI personnel conducting surveillance. The FBI's ability to recognize and its effectiveness at countering these counter-surveillance techniques have not been publically disclosed. Revealing the FBI ability to recognize and adapt to the deployment of counter-surveillance techniques would reveal key FBI surveillance techniques and best practices. This would allow criminals to predict the FBI's responses and strategies when conducting surveillance, and enable these criminals to avoid detection and disruption of their criminal activities by the FBI through FISUR. As releasing this information concerning counter-surveillance techniques would enable criminals to detect and potentially deter FBI FISUR, and more easily circumvent the law, this information exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Sensitive Terrorism Financing Investigative Techniques

(130) The pending files at issue contain descriptions of FBI techniques for investigating

terrorism financing. This information has not been released publically by the FBI. Investigating how money is funneled to terrorists/terrorist organizations has historically been a very effective means for the FBI to disrupt international terrorist organizations and the activities of individual terrorists. Revealing these techniques would reveal the scope of the FBI's capabilities to obtain and analyze financial data, and how this data can be utilized to investigative/disrupt terrorist activities. Releasing this information would be extremely detrimental to the FBI's use of these terrorism financing investigative techniques. If this information were made public, terrorists would be able to structure their financial activities/money laundering efforts in a manner which avoids detection and/or disruption by the FBI and other law enforcement agencies. This would allow these terrorists to fund violent behavior, across the globe, unimpeded. Release would undoubtedly enable terrorists to circumvent the laws of the United States, the laws of other nations throughout the world, and international law; therefore, this information is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

Sensitive Intelligence Databases

(131) The pending files at issue contain descriptions of numerous FBI internal databases utilized to house and disseminate accumulated investigative intelligence information. The existence of these databases and the manner in which they are utilized by the FBI in its investigations are not publicly known. The relative utility of these databases could be diminished if their existence the FBI's uses of the information they contain were released. Such a release would facilitate the accumulation of information by investigative subjects regarding circumstances under which information from the databases was used or requested, and the

usefulness to law enforcement of specific information obtained. This would enable criminals to educate themselves about what types of data are useful to the FBI in its investigations and therefore allow these individuals to deprive the FBI of these types of data. Over time, this could greatly diminish the FBI's ability to obtain, house, and query useful intelligence information, enabling criminals to circumvent the FBI's ability to detect and/or disrupt criminal behavior through the use of these databases; therefore, this information concerning sensitive intelligence databases is exempt from disclosure pursuant to FOIA Exemption (b)(7)(E).

DOCUMENTS REFERRED TO OTHER GOVERNMENT AGENCIES ("OGAs") FOR COORDINATION WITH THE FBI

(132) The FBI also identified pages, some in their entireties and some in part, containing information and/or equities originating with an OGA in the non-7A responsive material (Part I). In accordance with DOJ regulations, 28 C.F.R. § 16.4(c), the FBI coordinated with this OGA with equities in these documents to determine how that OGA wanted the FBI to treat its information contained within the responsive FBI documents.

Department of Justice – Civil Rights Division ("CRM")

(133) On May 13, 2015, the FBI sent 14 pages to CRM for coordination. These pages are identifiable as Todashev-1055-1068. On May 14, 2015, the FBI was notified that CRM determined that some of the information should be withheld in part[41] and some in full[42] pursuant

[41] Bates pages Todashev-1055 & 1058 were released in part per consultation with CRM.

[42] Bates pages Todashev-1056-1057 & 1059-1068 were withheld in full per consultation with CRM.

to 5 U.S.C. § 552(b)(5). The FBI addressed these pages in its initial releases of responsive material on May 1, 2015 and June 1, 2015 respectively. See ¶¶ 13-14, *supra*. Upon re-review for Vaughn code applicability, the FBI contacted CRM again on May 10, 2017. CRM advised that its information could now be released; therefore the information on these 14 pages attributable to CRM has been released in full with minor redactions per FBI pursuant to FOIA Exemptions (b)(6) and (b)(7)(C). Accordingly, the FBI is releasing Todashev-1055-1059 in part and Todashev-1060-1068 in full. See ¶ 15, *supra*.

PART II

Application of Exemption (b)(7)(A) to Withhold In Full Records From Pending Investigations

EXEMPTION (b)(7)(A) – PENDING ENFORCEMENT PROCEEDINGS

(134) The FBI applied FOIA Exemption (b)(7)(A) to withhold in full one main file, four cross references, one sub-file, and numerous serials from a large, multi-subject file, all pertaining to Ibragim Todashev. First, as previously demonstrated, these are law enforcement records compiled during criminal (international terrorism) investigations of Ibragim Todashev and/or others. Second, the records are from and/or pertain to pending or prospective investigations or prosecutions. Finally, the FBI has determined that release of the records would interfere with potential law enforcement proceedings. This determination of interference extends to the volume of responsive records because such information would reveal the scope and extent of the FBI's investigations, which would interfere with such ongoing proceedings.

TYPES OF DOCUMENTS

(135) Providing any further detailed document-by-document description or listing of the

records contained in the pending investigative files responsive to Plaintiff's request besides the information at paragraphs 135a-ll, *infra* would undermine the very interests that the FBI seeks to protect under Exemption (b)(7)(A), in addition to the other exemptions identified in this declaration *supra* as applying to those records. In order to protect these interests, the FBI has described the types of responsive records from the pending investigative files that are being withheld in full pursuant to FOIA Exemption (b)(7)(A). The pending investigative file contains the following types of documents:

(a) Interview Forms (Form FD-302[43]): FD-302s are internal FBI forms in which evidence is often documented, usually the results of FBI interviews. Such evidence and/or interview information may later be used as testimony or evidence in court proceedings/trials. Additionally, these evidence/interview forms are often incorporated in other FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(b) Form FD-1057 and Electronic Communications ("ECs"): FD-1057s and ECs replaced the traditional FBI correspondence (i.e., Memoranda and Letters) as the primary vehicle of correspondence within the FBI. The purpose of an EC is to communicate within the FBI in a consistent format that can be uploaded by the originating Division or office, transmitted, and downloaded by recipient Divisions or offices within the FBI's internal computer network. These forms are often utilized to record and disseminate intelligence/investigative information and for general investigation administration purposes.

[43] Forms designated "FD-" are FBI-created forms.

(c) Documents Implementing Sensitive Investigative Technique: These documents were utilized to implement a specific, sensitive, investigative technique. Describing these documents further would reveal this technique or sensitive data concerning this technique.

(d) FD-1054, 1055 and other Surveillance Logs: These types of documents are utilized to document physical surveillance ("FISUR") of investigative subjects. These surveillance logs include subjects/activities of subjects observed, the times these observations occurred, and the FBI personnel conducting the FISUR. These surveillance logs are often used as evidence, are incorporated in other FBI documents which disseminate intelligence/investigative information, and are utilized to set leads in furtherance of the FBI's investigative efforts.

(e) FD-704 Payment Requests: FD-704s are used to request payment to implement particular techniques or reimburse FBI units/squads/employees who their own funds to implement particular techniques.

(f) FD-888 Law Enforcement Operations Orders: FD-888s are utilized by FBI personnel to implement effective law enforcement operations. These forms document operation specifics, including objectives, suspects/targets, dates, times, equipment used, safety precautions, and the FBI/law enforcement personnel involved.

(g) Operation Plans: Similar to FD-888s, these documents are utilized by FBI personnel to plan and conduct effective law enforcement operations. These forms document operation specifics, including objectives, suspects/targets, dates, times, equipment used, safety precautions, and the FBI/law enforcement personnel involved.

(h) FBI Administrative Forms concerning 1A/1B Sections: These

administrative forms act as tables of contents in that they describe sections of a file in which certain types of documents are separately filed. These sections are usually designated in alphabetical order as 1A, 1B, etc. The types of documents filed in 1As/1Bs can include handwritten notes of interviews, photographs, and other various evidentiary documents.

(i) FD-340 - 1A Envelopes: These envelopes are used to organize and store documents that need to be stored separately from the FBI file to which they are attached, due to their size. They usually contain handwritten notes of interviews, photographs, and other various evidentiary documents.

(j) Court Documents: These are documents that have been filed with a court or otherwise made part of the court record.

(k) Photographs: This category consists of photographs taken and or collected in the course of the FBI investigations.

(l) Handwritten Interview Notes: These are the original handwritten notes of FBI personnel who conducted interviews in the course of FBI investigations. These notes are almost always transposed into FD-302s and are utilized by the FBI in the same manner.

(m) FD-941 – Consent to Search Forms: These documents were provided to and signed by individuals who consented to FBI searches of their persons/property.

(n) Random Evidentiary Documents: This category consists of any random evidentiary documents that were gathered during the course of FBI investigations. The information in these documents is often incorporated in other FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's

investigative efforts.

(o) Copies of Digital Evidence: This category consists of photocopies of digital evidence (CDs, DVDs).

(p) Interview Audio/Video: This category consists of audio/video recordings of interviews. Like FD-302s, this information may later be used as testimony or evidence in court proceedings/trials. Additionally, the results of these interviews are often incorporated in other FBI documents which disseminate intelligence/investigative information, and are utilized to set leads in furtherance of the FBI's investigative efforts.

(q) FD-5 Serial Charge Outs: These are administrative documents that explain why certain serials have been removed/replaced within FBI files.

(r) Internet Printouts: These documents consist of information that was located and printed form public websites. Though gathered from public source, this type of information can be treated as evidentiary, can be incorporated in documents disseminating investigatory information, and can be used to set leads in order to further FBI investigations.

(s) Computer/Telephone Examination Documents/Evidence: This category consists of evidence gathered and any reports resulting from analyses of computers, telephones, and similar digital media. These types of evidence can be used as evidence in court proceedings, are often incorporated in other FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(t) FD-472 Consent to Monitor: These forms are signed by individuals to document their consent to the FBI monitoring their communications with third parties.

(u) State and Local Law Enforcement Documents: This category consists of documents provided to the FBI by state and local law enforcement agencies. These documents can be used as evidence in court proceedings, are often incorporated in other FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(v) Internal Electronic Mail Messages (E-mails): These documents consist of E-mails between FBI personnel discussing investigative matters.

(w) FBI Records Checks: These documents are printout of queries of internal FBI databases. These documents are often incorporated in other FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(x) Federal Grand Jury Subpoenas/Subpoenaed Information: These documents consist of Federal Grand Jury Subpoenas and the documents collected as a result of these subpoenas. This information can be used as evidence in Grand Jury proceedings or other court proceedings. This information can also be incorporated in FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(y) FBI Translations: These are translations of foreign language documents, conducted by FBI linguists. This information can be used as evidence in court proceedings, can be incorporated in FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(z) Memorandum: These are ordinarily communications to DOJ officials, from one person to another at FBIHQ, or from one person to another within an FBI field office. They serve to assist in the overall supervision of a case by summarizing pertinent details of an investigation.

(aa) Other Government Agency Information: These are documents provided to the FBI by other federal government agencies. This information can be incorporated in FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(bb) Miscellaneous Administrative Documents: This category consists of all informal, internal documents utilized to administer FBI coordination and investigation administration.

(cc) FD-1036 – Sentinel Import Forms: These are administrative forms attached to documents that are imported into the FBI's case administrative system, Sentinel.

(dd) ORION Information Packages: The FBI's Operation Response and Investigative Online Network ("ORION"), is a crisis information management system that allows the FBI, federal, state, local and tribal law enforcement agencies to coordinate/share information during crises, special events, or critical incidents. These ORION information packages are utilized to disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI and other law enforcement agencies' investigative efforts.

(ee) Informal Intelligence Write-ups: This category consists of informal, intelligence documents written to document/disseminate relevant intelligence information.

(ff) Foreign Government Information: These are documents that were provided to the FBI by foreign governments. This information within these documents can be incorporated in FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(gg) FBI Letters: The FBI letter is the formal correspondence format used to communicate with non-FBI entities, including but not limited to, other federal agencies, other non-federal law enforcement agencies, commercial businesses, and/or private citizens. Its format is identical to business letters utilized by commercial agencies, except that it contains the FBI Seal at the top of the first page.

(hh) Laboratory Forms/Reports: These are documents prepared by the FBI with a description of material submitted to the laboratory, or reports prepared by FBI laboratory personnel documenting their findings following testing of material submitted to the laboratory. This information can be used as evidence in court proceedings, can be incorporated in FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(ii) FD 1023 – CHS Reporting Documents: These standard forms document reporting to the FBI by Confidential Human Sources ("CHS"). This CHS provided information may later be used as testimony or evidence in court proceedings/trials. Additionally, this information can be incorporated in other FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(jj) ERT Casebooks: Evidence Response Teams ("ERTs") are teams of FBI personnel that are assembled to document/process evidence at crime scenes. These teams create "Casebooks" to organize their findings into a concise, informational package. This information can be used as evidence in court proceedings, can be incorporated in FBI documents which disseminate intelligence/investigative information, and can be utilized to set leads in furtherance of the FBI's investigative efforts.

(kk) Teletypes: Teletypes are an electronic means of disseminating law enforcement/intelligence information between FBI field offices, FBIHQ and the United States intelligence and law enforcement agencies.

(ll) Sentinel Leads: These are investigative directives, disseminated internally between FBI personnel, through Sentinel.

PENDING LAW ENFORCEMENT PROCEEDINGS

(136) Material responsive to Plaintiff's request is located in files of ongoing investigations. Release of any information, other than public source information from these files, could reasonably be expected to interfere with these pending criminal law enforcement proceedings, as well as potential enforcement proceedings such as spin-off investigations and/or prosecutions that may result from the investigations. The In Camera, Ex Parte Declaration of David Hardy, provides more detailed information about the enforcement proceedings. These pending investigative files contain public source information, which was processed and released to Plaintiff. Until the potential and pending enforcement proceedings are concluded and resolved, however, no additional information contained in these files can be released to Plaintiff

without interfering in pending or prospective enforcement proceedings.

REASONABLE EXPECTATION OF INTERFERENCE

(137) In processing requests under the FOIA, the FBI has established procedures allowing it to implement the FOIA as efficiently as possible. When a request is received for records related to an ongoing FBI investigation, the FBI commonly asserts FOIA Exemption (b)(7)(A) in response to such a request, but the FBI segregates and releases information related to the pending investigation where release would not jeopardize future investigative or prosecutive efforts. The FBI's review of the responsive records for the preparation of this declaration revealed that aside from the public source material previously released to Plaintiff, no additional material from the pending files can be released without jeopardizing further investigation and/or prosecutive efforts.

(138) Any release of information from these files to Plaintiff would be premature and likely to cause harm. While the pending records at issue pertain to Ibragim Todashev, a deceased individual, the records, by their nature, also pertain to other living targets of investigative interest who are/were associated with Ibragim Todashev, and/or would reveal the scope of pending FBI investigative efforts. Release of these records would allow targeted individuals to critically analyze documents concerning these investigations. Such individuals possess the unique advantage of knowing the details surrounding the potential criminal activities, the identities of potential witnesses, and the direct and circumstantial evidence of the potential criminal activities. These individuals could therefore use the released information to their advantage to destroy evidence, intimidate potential witnesses, and/or evade the FBI's investigative efforts. In this

regard, the following potential harms from the release of information contained in these documents exist:

a. the identification of individuals, sources, and potential witnesses who possess information relative to the investigation and possible harm to, or intimidation of these individuals;

b. the use of released information to counteract evidence developed by investigators, alter or destroy potential evidence or create false evidence;

c. the use of information released to uncover the government's trial strategy; and

d. the use of released information by any subject of the investigations to assess the likelihood that he or she may be prosecuted and/or convicted in connection with this investigation.

(139) Furthermore, the release of this information could allow third parties to interfere with the pending proceedings by harassment, intimidation, and creation of false evidence by dispensing extraneous facts discussed during FBI investigations. Once a release is made to Plaintiff under the FOIA, Plaintiff's use and dissemination of the information to third parties is unrestricted.

Functional Categories of Information Protected Under FOIA Exemption (b)(7)(A)

(140) The FBI has grouped the records in the responsive main files and cross reference record into functional categories for purposes of demonstrating why the information is exempt from disclosure under FOIA Exemption (b)(7)(A). Each responsive document that was withheld falls into one or more of the functional categories described in the following paragraphs. For

example, one document may serve several purposes and may contain multiple categories of information, such as witness statements, administrative directions or evidentiary materials. This document could, therefore, be included in multiple categories as could the information contained within the document. Here, the functional categories include:

A. ***Evidentiary/Investigative Materials***: This category includes copies of records or evidence, and derivative communications discussing or incorporating evidence. A derivative communication describes, verbatim or in summary, the contents of the original record, how it was obtained, and how it relates to the investigation. Other derivative communications report this information to other FBI Field Offices or other law enforcement agencies, either to advise them of the progress of the investigation, or to elicit their assistance in handling investigative leads. The following subparagraphs describe the types of evidentiary material in the responsive records and the anticipated harm that could reasonably result from the release of such materials.

i. Information Concerning Physical and Documentary Evidence:

Information concerning physical and documentary evidence in this file may include records obtained through and/or summarizing information gathered through searches, seizures, surveillance, confidential source/witness interviews, Federal Grand Jury subpoenas, laboratory reports, and any other law enforcement/intelligence gathering activities. To more fully describe these records could reasonably lead to disclosure of the nature of the pending investigative efforts/programs to which these records pertain. Such a disclosure could be detrimental to success of the pending and prospective enforcement proceedings by permitting

subjects to estimate the scope of the FBI's investigation and judge whether their activities are likely to be detected; allowing investigative subjects to discern the FBI's investigative strategies and employ countermeasures to avoid detection and disruption by law enforcement; and/or allow investigative targets formulate strategies to contradict evidence to be presented in Court proceedings.

ii. Exchange of Information with Foreign Governments: Release of the FBI's exchanges of information with Foreign Governments in relation to the documents at issue could cause four distinct harms to the pending investigative efforts to which these records pertain. First, release of this type of information would reveal FBI intelligence gaps by revealing the types of information the FBI desired to obtain from friendly foreign law enforcement/intelligence agencies. Criminals could use this information to judge whether or not the FBI has detected their criminal behaviors and/or whether or not they need to destroy evidence/deploy countermeasures to avoid further investigative efforts. Second, revealing the types of information shared between the FBI and its foreign partners would reveal the types and volume of information shared between the FBI and certain foreign governments and thus the extent to which traveling internationally benefits criminals/criminal organizations involved in the pending investigations. Third, releasing this type of information would also reveal the extent and limitations of the FBI's foreign partners. Whether releasing information concerning these foreign partners' efforts to elicit information from the FBI and/or any relevant information provided to the FBI by these foreign governments, release of these foreign governments' information would provide criminals with details concerning the scope,

strengths, and weaknesses of these foreign governments' investigative efforts. This would allow criminals to judge whether, when, and how their criminal activities have and/or will come under scrutiny by the FBI and friendly foreign law enforcement/intelligence agencies. Fourth, information shared between the FBI and its foreign partners is done so with the understanding that the FBI's relationships with these foreign agencies and the information shared will remain confidential. Revealing this information would damage these relationships, potentially staunch the free-flow of pertinent investigative information between the FBI and its foreign partners, and hinder the FBI's ability to investigate any international crimes under scrutiny in the pending investigative efforts at issue.

iii. Exchange of Information Between Various Local, State, and/or Federal Agencies: Release of records documenting and detailing the exchange of information among law enforcement partners will disclose investigative information developed by various agencies that have cooperated with and provided information and records to the FBI in this pending investigation. This information was gathered to help identify subjects, suspects or other individuals of potential investigative interest and to assist in locating witnesses and/or confidential sources. Inherent in this cooperative effort is the mutual understanding that information provided to the FBI by those agencies will not be prematurely released. Moreover, release of this information would identify the investigative interest in particular individuals as well as subject witnesses and confidential sources to potential harassment, intimidation and physical or mental harm.

iv. Confidential Source and Witness Statement: Confidential source and

witness statements are one of the principal tools used in proving the facts that form the basis for a prosecution. These statements contain information obtained from confidential informants, records custodians, and other third party individuals who have knowledge of the criminal (international terrorism) activities at issue in the FBI investigations. If this information was released, the witnesses and/or confidential sources that have chosen to cooperate with law enforcement could be subjected to retaliation, intimidation, or physical or mental harm. This could have a chilling effect on the future investigative efforts and prosecutions in this and other cases inasmuch as potential witnesses and/or confidential sources might fear exposure and reprisals from the subjects of these investigations.[44] Implicit in conducting interviews in investigations of this nature is the notion that an individual's identity and the information provided by them will be afforded confidentiality. The FBI goes to great lengths to protect and maintain an individual's confidentiality since it is an integral part of a successful investigation and prosecution. The release of witness statements and confidential source statements would disrupt and harm future investigative and/or prosecutive actions.

B. ***Administrative Materials:*** Materials that fall into this category include items such as case captions, serial numbers, identities of FBI field offices involved, dates of investigation, and detailed instructions designed to ensure that investigative procedures are conducted within the appropriate FBI and DOJ guidelines. The following subparagraphs describe the types of administrative materials contained in this file and the anticipated harm that

[44] Individuals cooperating with law enforcement in these types of cases have been subject to harassment and have been threatened with harm up to and including death threats when their cooperation has become public.

could reasonably result from the release of such materials. In many instances, administrative information is contained in correspondence or documents that also fall into other categories. Therefore, release of details with respect to this category of information would also reveal the investigative interests of the FBI and could enable suspects to discern a "road map" of the investigations.

i. Reporting Communications: These communications permit the FBI and/or other agencies to monitor the progress of the investigation and to facilitate its conduct. These communications may reveal or confirm the cooperation of other local, state, or federal agencies in the investigation. They are replete with detailed information about the investigative activities as well as detailed information about potential witnesses and confidential sources to be interviewed. Additionally, they contain background information about third party individuals, the origin of pertinent information that ties them to the investigation, their connection with the subjects, and their relationship with the pending investigation. The release of this information would reveal the investigative steps taken to obtain witness and confidential source interviews, techniques and investigative methods used to compile and/or solicit information from various sources, and the perceived weaknesses in the investigation. The release of this information would reveal the nature and scope of the pending investigations.

ii. Administrative Instructions: This type of information, whether it originates in communications from DOJ, the FBI, or other domestic or foreign law enforcement agencies, if released to a knowledgeable person, would disclose specific investigative procedures and strategies employed in this investigation. Release of this information would thus permit the

subjects of these investigations to anticipate and possibly alter or negate incriminating evidence which could be used in future prosecutions/investigative efforts. Specific examples of these instructions include the setting out of investigative guidelines and requests for specific investigative inquiries at various FBI field offices or other government agencies. These instructions are commonly referred to as "investigative leads" and are set forth throughout the course of FBI investigations.

iii. Miscellaneous Administrative Documents: These types of materials were used throughout this investigation for many routine purposes. While these materials are not solely applicable to this investigation, they were adapted or used in such a manner so as to contain information of investigative value. An example is the envelope used to store records obtained from a confidential source. While the envelope is not specific to this investigation, handwritten notations on the envelope identify dates, places, and the persons who provided the records. The disclosure of these materials could harm the investigation by providing details which, when viewed in conjunction with knowledge possessed by the subjects, could provide information useful in identifying witnesses, investigative strategies, legal information, and items of evidence.

C. ***Public Source Materials:*** The FBI segregated and released one category of information in the responsive pending files – public source information, such as newspaper/magazine articles – because it was determined that such information would not interfere with any pending or prospective enforcement proceedings. The FBI released to Plaintiff approximately 63 pages in full of such information Bates Stamped Todashev-1087-1149 by letters

dated May 1, 2015 and June 1, 2015. *See* ¶ 13-14, *supra.* With the exception of this public source information, there is no other reasonably segregable portion of any document that can be released from the pending investigative files responsive to Plaintiff's request.

ASSERTION OF UNDERLYING EXEMPTIONS UNDER THE FOIA

(141) With the exception of public source information and the files pertaining to the shooting death of Ibragim Todashev, the files responsive to Plaintiff's request have been denied in their entirety pursuant to FOIA Exemption (b)(7)(A). In light of the D.C. Circuit's ruling in Maydak v. U. S. Department of Justice, 218 F.3d 760 (D.C. Cir. 2000), however, Exemptions (b)(1), (b)(3), (b)(5), (b)(6), (b)(7)(C), (b)(7)(D), and (b)(7)(E) of the FOIA are also being asserted as additional basis for protecting information in the records withheld in full pursuant to FOIA Exemption (b)(7)(A) (as described in this Part II at paragraphs 134-140C, *supra*).

(142) As noted above in Parts I & II at paragraphs 27-133 & 134-140C, *supra* respectively, the FBI asserts all applicable underlying FOIA exemptions in both the responsive records from the FBI's investigation into the shooting death of Ibragim Todashev by an FBI Special Agent ("SA") processed and released by the FBI; and those responsive records exempted in full pursuant to FOIA Exemption (b)(7)(A) in the Investigative/Evidentiary and Administrative records discussed above. Accordingly, the FBI is asserting FOIA Exemption (b)(1) to protect classified information (*See* ¶¶ 31-58, *supra)*; FOIA Exemption (b)(3) to protected statutory information (*See* ¶¶ 59-68, *supra)*; FOIA Exemption (b)(5) to protect privileged information (*See* ¶¶ 69-72, *supra)*; FOIA Exemptions (b)(6) and (b)(7)(C) to protect information whose release would warrant a clearly unwarranted invasion of privacy and unwarranted invasion of personal

privacy (*See* ¶¶ 75-85, *supra)*; FOIA Exemption (b)(7)(A) to protect pending enforcement proceedings (*See* ¶¶ 86-89, *supra);* FOIA Exemption (b)(7)(D) to protect confidential source information (*See* ¶¶ 90-101, *supra)*; and FOIA Exemption (b)(7)(E) to protect numerous investigative techniques and procedures (*See* ¶¶ 102-131, *supra)*. With regard to Part II, at this time public disclosure of more detailed information on the application of exemptions would undermine the very interests the FBI seeks to protect through its assertion of Exemption (b)(7)(A) because it could reasonably be expected to reveal the nature, scope, focus, and conduct of the pending investigation and any resulting prosecutions.

SEGREGABILITY

(143) All documents were processed to achieve maximum disclosure consistent with the access provisions of the FOIA. Every effort was made to provide Plaintiff with all material in the public domain and with all reasonably segregable portions of releasable material. No reasonably segregable, nonexempt portions were withheld from Plaintiff.

(144) As discussed in ¶ 4 *supra*, there were 1,148[45] responsive pages identified: 378 Released in Full ("RIF"), 418 Released in Part ("RIP"), and 352 Withheld in Full ("WIF"). Each of these categories is discussed below to further address segregability.

A. Pages RIF. Following the segregability review, RIDS determined that 369 pages could be released in full without redaction as there was no foreseeable harm to an interest protected by a FOIA exemption.

B. Pages RIP. Following the segregability review, RIDS determined that 415 pages

[45] *See* fn. 1, *supra.*

could be released in part with redactions per the identified FOIA exemptions herein. These pages comprise a mixture of material that could be segregated for release and material that was withheld as release would trigger foreseeable harm to one or more interests protected by the cited FOIA exemptions on these pages.

C. Pages WIF. Following the segregability review, RIDS determined that 364 pages were required to be withheld in their entirety. Of these, 46 pages were withheld in their entirety because they were duplicative of other pages[46], and 318 pages were withheld in their entirety because RIDS determined that all information on these pages was fully covered by FOIA Exemptions[47]. RIDS determined that any non-exempt information on these pages was so intertwined with exempt material, that no information could be reasonably segregated for release. Any further segregation of this intertwined material would employ finite resources only to produce disjointed words, phrases, or sentences, that taken separately or together, would have minimal or no informational content.

CONCLUSION

(145) The FBI performed adequate and reasonable searches for responsive records;

---

[46] Bates pages Todashev-53-68, 192, 544, 808, 840-841, 931, 959-961, & 1024-1044 were withheld in their entirety as duplicative of other pages.

[47] Bates pages Todashev-1, 84, 186, 194-200, 206-218, 251, 258, 261-276, 278-290, 293, 299, 301-303, 305-307, 311, 313-314, 316-317, 319-458, 461-488, 492-497, 500-528, 545, 573-574, 581-582, 597, 612, 623, 666-668, 671, 677-680, 684-687, 691-701, 736-739, 765, 811-813, 835, 843-844, 846, 848, 996, 1002, 1023 were withheld in their entirety because RIDS determined that all information on these pages was fully covered by FOIA Exemptions (b)(6) and (b)(7)(A), (b)(7)(C), and (b)(7)(E).

processed all such records and released all reasonably segregable non-exempt information from documents responsive to Plaintiff's FOIA request that are subject to FOIA. The FBI processed the records under the access provisions of the FOIA to achieve maximum disclosure.

(146) The FBI identified 1,086 pages of responsive records that it processed for release with redactions based on FOIA Exemptions (b)(1), (b)(3), (b)(6), (b)(7)(A), (b)(7)(C), (b)(7)(D) and (b)(7)(E) (Part 1). The FBI carefully examined the documents and determined that the information withheld from Plaintiff in this case, if disclosed: would reveal classified and statutorily protected information; would cause a clearly unwarranted invasion of the personal privacy, or could reasonably be expected to constitute an unwarranted invasion of personal privacy; and would disclose techniques and procedures for law enforcement investigations. No reasonably segregable nonexempt portions of these pages were withheld from Plaintiff.

(147) The FBI search also located responsive records part of ongoing investigations and concluded that almost all responsive records from those pending investigations could not be released at this time without adversely affecting the investigations or any resulting prosecutions, and therefore withheld them pursuant to FOIA Exemption (b)(7)(A) (Part II). The FBI concluded, however, that 63 pages of public source materials from that pending investigation file could be released without adversely affecting the investigation and in fact released those pages to Plaintiff. Aside from these 63 pages of public source materials, no other nonexempt information existed that could be reasonably segregated without adversely affecting the pending investigation and any resulting enforcement proceedings. In these records withheld in full pursuant to FOIA Exemption (b)(7)(A), the FBI also applied FOIA Exemptions (b)(1), (b)(3), (b)(5), (b)(6),

(b)(7)(C), (b)(7)(D), and (b)(7)(E) to protect classified information; information prohibited from disclosure by Rule 6(e), and the BSA; information that if disclosed, would cause a clearly unwarranted invasion of the personal privacy, or could reasonably be expected to constitute an unwarranted invasion of personal privacy; information that, if disclosed, could reasonably be expected to disclose the identities of confidential sources and the information they provided; and information, if disclosed, would disclose techniques and procedures for law enforcement investigations.

(148) After extensive review of the documents at issue, I have determined that there is no further non-exempt information that can be reasonably segregated and released without revealing exempt information.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct, and that Exhibits A through I attached hereto are true and correct copies.

Executed this 15th day of May 2017.

DAVID M. HARDY
Section Chief
Record/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Winchester, Virginia

FOR OFFICIAL USE ONLY

Updated 2/19/2009

JOINT TERRORISM TASK FORCE

STANDARD MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(the "Participating Agency")

PREAMBLE

The policy of the United States with regard to domestic and international terrorism is to deter, defeat, and respond vigorously to all terrorist attacks on our territory and against our citizens, or facilities. Within the United States, the Department of Justice, acting through the Federal Bureau of Investigation (FBI), is the lead agency domestically for the counterterrorism effort.

In order to ensure that there is a robust capability to deter, defeat, and respond vigorously to terrorism in the U.S. or against any U.S. interest, the FBI recognizes the need for all federal, state, local, and tribal agencies that are involved in fighting terrorism to coordinate and share information and resources. To that end, the FBI believes that the creation of the FBI National Joint Terrorism Task Force (NJTTF) and Joint Terrorism Task Forces (JTTFs) embodies the objectives of the U.S. policy on counterterrorism as set forth in Presidential Directives.

FBI policy for the NJTTF and JTTFs is to provide a vehicle to facilitate sharing FBI information with the intelligence and law enforcement communities to protect the United States against threats to our national security, including international terrorism, and thereby improve the effectiveness of law enforcement, consistent with the protection of classified or otherwise sensitive intelligence and law enforcement information, including sources and methods. All NJTTF and JTTF operational and investigative activity, including the collection, retention and dissemination of personal information, will be conducted in a manner that protects and preserves the constitutional rights and civil liberties of all persons in the United States.

This Memorandum of Understanding (MOU) shall serve to establish the parameters for the detail of employees (Detailees or members) from the Participating Agency to the FBI-led JTTFs in selected locations around the United States.

FOR OFFICIAL USE ONLY
This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

I. PURPOSE

A. The purpose of this MOU is to outline the mission of the JTTF, and to formalize the relationship between the FBI and the Participating Agency; in order to maximize cooperation and to create a cohesive unit capable of addressing the most complex terrorism investigations.

B. The MOU specifically represents the agreement between the FBI and the Participating Agency, which will govern the process by which employees of the Participating Agency are detailed to work with the FBI as part of the JTTF.

C. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the U.S., or the officers, employees, agents or other associated personnel thereof.

II. MISSION

The mission of the JTTF is to leverage the collective resources of the member agencies for the prevention, preemption, deterrence and investigation of terrorist acts that affect United States interests, and to disrupt and prevent terrorist acts and apprehend individuals who may commit or plan to commit such acts. To further this mission, the JTTF shall serve as a means to facilitate information sharing among JTTF members.

III. AUTHORITY

Pursuant to 28 U.S.C. § 533, 28 C.F.R. § 0.85, Executive Order 12333, as amended, National Security Presidential Directive (NSPD) 46/ Homeland Security Presidential Directive (HSPD) 15 and Annex II thereto, the FBI is authorized to coordinate an intelligence, investigative, and operational response to terrorism. By virtue of that same authority, the FBI formed JTTFs composed of other federal, state, local, and tribal law enforcement agencies acting in support of the above listed statutory and regulatory provisions.

[*Participating agencies may include applicable authority for entering into this MOU.*]

IV. CONTROLLING DOCUMENTS

A. Since the JTTF operates under the authority of the Attorney General of the United States, all JTTF participants must adhere to applicable Attorney General's Guidelines and directives, to include the following; as amended or supplemented:

**This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.**

1. Attorney General's Guidelines for Domestic FBI Operations;

2. Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations;

3. Attorney General's Guidelines Regarding Prompt Handling of Reports of Possible Criminal Activity Involving Foreign Intelligence Sources;

4. Attorney General Memorandum dated March 6, 2002, titled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI";

5. Attorney General's Guidelines Regarding the Use of Confidential Informants;

6. Attorney General's Guidelines on the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions;

7. Attorney General's Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation; and

8. Memorandum from the Deputy Attorney General and the FBI Director re: Field Guidance on Intelligence Sharing Procedures for [Foreign Intelligence] and [Foreign Counterintelligence] Investigations (December 24, 2002).

B. All guidance on investigative matters handled by the JTTF will be issued by the Attorney General and the FBI. The FBI will provide copies of the above-listed guidelines and any other applicable policies for reference and review to all JTTF members. Notwithstanding the above, this MOU does not alter or abrogate existing directives or policies regarding the conduct of investigations or the use of special investigative techniques or controlled informants. The FBI agrees to conduct periodic briefings of the member agencies of the JTTF pursuant to all legal requirements and FBI policies.

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

V. STRUCTURE AND MANAGEMENT OF THE TASK FORCE

A. MEMBERS

1. Each JTTF shall consist of a combined body of sworn and non-sworn personnel from the FBI and each Participating Agency. This MOU shall apply to Participating Agencies that join the JTTF subsequent to execution of this agreement.

B. PROGRAM MANAGEMENT, DIRECTION, AND SUPERVISION

1. In order to comply with Presidential Directives, the policy and program management of the JTTFs is the responsibility of FBI Headquarters (FBIHQ). The overall commander of each individual JTTF will be the Special Agent in Charge (SAC) or Assistant Director in Charge (ADIC), if assigned, of the FBI's local Field Division. The operational chain of command beginning at the highest level, in each FBI Field Division will be as follows: ADIC if assigned, SAC, Assistant Special Agent in Charge (ASAC), and Supervisory Special Agent [JTTF Supervisor].

2. Each FBI ADIC/SAC, through his or her chain-of-command, is responsible for administrative and operational matters directly associated with the Division's JTTF(s). Operational activities will be supervised by FBI JTTF Supervisors. Staffing issues are the responsibility of the FBI chain of command.

3. All investigations opened and conducted by the JTTF must be conducted in conformance with FBI policy, to include the above stated Controlling Documents. Each FBI ADIC/SAC, through his or her chain-of-command, will ensure that all investigations are properly documented on FBI forms in accordance with FBI rules and regulations. Any operational problems will be resolved at the field office level. Any problems not resolved at the field office level will be submitted to each agency's headquarters for resolution.

4. Each Participating Agency representative will report to his or her respective agency for personnel administrative matters. Each Participating Agency shall be responsible for the pay, overtime, leave, performance appraisals, and other personnel matters relating to its employees detailed to JTTFs. As discussed later herein at Paragraph XI, the FBI and the Participating Agency may provide for overtime reimbursement by the FBI by separate written agreement.

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

5. Each JTTF member will be subject to the personnel rules, regulations, laws, and policies applicable to employees of his or her respective agency and also will adhere to the FBI's ethical standards and will be subject to the Supplemental Standards of Ethical Conduct for employees of the Department of Justice. Where there is a conflict between the standards or requirements of the Participating Agency and the FBI, the standard or requirement that provides the greatest organizational protection or benefit will apply, unless the organizations jointly resolve the conflict otherwise.

6. JTTF members are subject to removal from the JTTF by the FBI for violation of any provision of this MOU, the FBI's ethical standards, the Supplemental Standards of Ethical Conduct for employees of the Department of Justice, or other applicable agreements, rules, and regulations.

7. The FBI maintains oversight and review responsibility of the JTTFs. In the event of an FBI inquiry into JTTF activities by an investigative or administrative body, including but not limited to, the FBI's Office of Professional Responsibility or the FBI's Inspection Division, each Participating Agency representative to the JTTF, may be subject to interview by the FBI.

C. PHYSICAL LOCATION AND SUPPORT:

1. The FBI will provide office space for all JTTF members and support staff. In addition, the FBI will provide all necessary secretarial, clerical, automation, and technical support for the JTTF in accordance with FBI guidelines and procedures. The FBI will provide all furniture and office equipment. Participating agencies may bring office equipment or furniture into FBI space with the approval of the FBI JTTF Supervisor and in compliance with FBI regulations.

2. The introduction of office equipment and furniture into FBI space by Participating Agencies is discouraged, as any such material is subject to examination for technical compromise, which may result in its being damaged or destroyed.

VI. SECURITY PROGRAM

A. CLEARANCES

1. State, local, and tribal members of the JTTFs, as well as appropriate supervisory personnel responsible for these individuals, must apply for and

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

receive a Top Secret/Sensitive Compartmented Information (TS/SCI) Security Clearance granted by the FBI. JTTF members from other federal agencies must obtain a Top Secret/SCI clearance from their agency and have this information passed to the FBI. No one will have access to sensitive or classified documents or materials or FBI space without a valid security clearance and the necessary "need-to-know." Pursuant to the provisions of Section 1.2 of Executive Order 12968, Detailees are required to have signed a nondisclosure agreement approved by the FBI's Security Division. Pursuant to federal law, JTTF members are strictly forbidden from disclosing any classified information to individuals who do not possess the appropriate security clearance and the need to know.

2. All JTTF management personnel must ensure that each participating JTTF officer or agent undertakes all necessary steps to obtain a TS/SCI clearance. Conversion of FBI counterterrorism and JTTF spaces to Sensitive Compartmented Information Facilities (SCIFs) is underway. This will require that all JTTF task force officers enhance their clearances to TS/SCI (SI, TK, Gamma, HCS-P).

3. Federal agency task force officers should contact their Security Officers and request and obtain the following SCI Clearances: SI, TK, Gamma, and HCS-P. If the parent agency refuses or is unable to provide the appropriate clearances, the FBI will request the task force officer's security file. If provided, the FBI will adjudicate SCI clearances. This action may involve a prohibitively long process and should be avoided.

4. Each Participating Agency fully understands that its personnel detailed to the JTTF are not permitted to discuss official JTTF business with supervisors who are not members of the JTTF unless the supervisor possesses the appropriate security clearance and the dissemination or discussion is specifically approved by the FBI JTTF Supervisor. Participating Agency heads will be briefed regarding JTTF matters by the SAC or ADIC, as appropriate, through established JTTF Executive Board meetings.

5. In accordance with the Director of Central Intelligence Directive (DCID) 6/4, entitled Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI), the FBI will implement protocols to ensure Special Agent (SA) and Task Force Officers (TFO) assigned to Joint Terrorism Task Forces (JTTF) in the field and the National Joint Terrorism Task Force (NJTTF) at FBI Headquarters - Liberty Crossing 1, are in compliance with stated directive. In order to comply with DCID 6/4, all JTTF personnel, including FBI and non-FBI

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

JTTF members and contractors who perform functions requiring access to FBI classified data networks and space, will be given counter-intelligence focused polygraphs. The FBI will recognize polygraph examinations conducted by outside federal agencies that meet the FBI's PSPP requirement. The FBI will make the final determination whether a polygraph examination meets the PSPP requirements.

6. All JTTF members must agree to submit to counter-intelligence focused polygraphs as part of the process for obtaining and retaining a Top Secret Security Clearance.

B. RESTRICTIONS ON ELECTRONIC EQUIPMENT

Personally owned Portable Electronic Devices (PEDs) including, but not limited to, personal digital assistants, Blackberry devices, cellular telephones, and two-way pagers are prohibited in FBI space unless properly approved. No personally owned electronic devices are permitted to operate within SCIFs as outlined in DCI Directive 6/9 and existing Bureau policy. All other non-FBI owned information technology and systems (such as computers, printers, fax machines, copiers, PEDs, cameras, and media including diskettes, CDs, tapes) require FBI approval prior to introduction, operation, connection, or removal from FBI spaces to include SCIFs. Additionally, if approved by the FBI Security Officer, these systems must operate in compliance with the FBI's policies, guidelines, and procedures.

VII. DEPUTATION

Non-federal members of the JTTF who are subject to a background inquiry and are sworn law enforcement officers will be federally deputized while detailed to the JTTF. The FBI will secure the required authorization for their deputation. Deputation of these individuals will ensure that they are able to assist fully in investigations in compliance with applicable federal statutes. On occasion, investigations may be conducted outside of the JTTF's assigned territory. Deputation will allow non-federal members of the JTTF to exercise federal law enforcement authority throughout the United States.

Under the terms of this MOU, all Participating Agencies agree that non-sworn personnel detailed to the JTTF will not : (1) participate in law enforcement activities, (2) carry a weapon; or (3) participate in the execution of search/arrest warrants.

VIII. STAFFING COMMITMENT

A. In view of the need for security clearances and continuity of investigators, all personnel detailed to the JTTF should be expected to be detailed for a period of at least two (2) years. This MOU imposes no maximum limit as to the time that any individual may remain a member of the JTTF. All non-FBI members of the JTTF

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

must adhere to the same rules and regulations as FBI employees with regard to conduct and activities while in FBI space, while operating FBI vehicles, and while conducting JTTF business. All Task Force members detailed from other federal agencies are responsible for maintaining an appropriate case load, as directed by JTTF management.

B. All investigators detailed to the JTTF will be designated either full-time or part-time. The operational needs of the JTTF require that any assignments to special details, or duties outside of the JTTF to full-time JTTF members be coordinated with the FBI JTTF Supervisor. Though each JTTF member will report to his or her respective Participating Agency for personnel matters, he or she will coordinate leave with the JTTF's FBI JTTF Supervisor.

C. During periods of heightened threats and emergencies, the JTTFs may be expected to operate 24 hours per day, seven days per week, for extended periods of time. To function properly, the JTTF depends upon the unique contributions of each Participating Agency. Accordingly, during these periods, each Participating Agency member will be expected to be available to support JTTF activities.

IX. RECORDS, REPORTS AND INFORMATION SHARING

A. All JTTF materials and investigative records, including any Memorandum of Understanding, originate with, belong to, and will be maintained by the FBI. All investigative reports will be prepared by JTTF personnel solely on FBI forms. All information generated by the FBI or the JTTF will be controlled solely by the FBI and may not be removed from FBI space without the approval of the JTTF Supervisor. Dissemination, access or other use of JTTF records will be in accordance with Federal law, Executive Orders, and Department of Justice and FBI regulations and policy, including the dissemination and information sharing provisions of the FBI Intelligence Policy Manual. As FBI records, they may be disclosed only with FBI permission and only in conformance with the provisions of federal laws and regulations, including the Freedom of Information Act, 5 U.S.C. Section 552, and the Privacy Act of 1974, 5 U.S.C. Section 552a, as well as applicable civil and criminal discovery privileges. This policy includes any disclosure of FBI information, including JTTF materials and investigative records, to employees and officials of a Participating Agency who are not members of a JTTF, which must be approved by the JTTF supervisor. All electronic records and information, including, but not limited to, systems, databases and media, are also regulated by FBI policy. JTTF members may request approval to disseminate FBI information from the JTTF Supervisor.

B. Each Participating Agency agrees to have its Detailees to the JTTF execute an FD-868, or a similar form approved by the FBI . This action obligates the Detailee,

**This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.**

who is accepting a position of special trust in being granted access to classified and otherwise sensitive information as part of the JTTF, to be bound by prepublication review to protect against the unauthorized disclosure of such information.

C. The participation of other federal, state, local, and tribal partners on the JTTF is critical to the long-term success of the endeavor. Articulating the level of effort for these partnerships is a key measure of the JTTF's performance. Accordingly, all task force members will be required to record their workload in the Time Utilization Recordkeeping (TURK) system used by the FBI.

X. COORDINATION

A. The Participating Agency agrees to not knowingly act unilaterally on any matter affecting the JTTF without first coordinating with the FBI. The parties agree that matters designated to be handled by the JTTF shall not knowingly be subject to non-JTTF or non-FBI intelligence, law enforcement, or operational efforts by the Participating Agency. Intelligence, law enforcement, and operational actions will be coordinated and cooperatively carried out within the JTTFs.

B. JTTF criminal investigative procedures will conform to the requirements for federal prosecution. It is expected that the appropriate United States Attorney, in consultation with the FBI and affected JTTF partners, will determine on a case-by-case basis whether the prosecution of cases will be at the federal or state level, based upon which would better advance the interests of justice.

XI. FUNDING

This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds. Even where one party has agreed (or later does agree) to assume a particular financial responsibility, written agreement must be obtained before incurring an expense expected to be assumed by another party. All obligations of and expenditures by the parties are subject to their respective budgetary and fiscal processes and availability of funds pursuant to all laws, regulations, and policies applicable thereto. The parties acknowledge that there is no intimation, promise, or guarantee that funds will be available in future years. The FBI and the Participating Agency may enter into a separate agreement to reimburse the Participating Agency for approved overtime expenses.

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

XII. TRAVEL

All JTTF-related travel of non-FBI personnel requires the approval of the appropriate JTTF Supervisor and Participating Agency authorization prior to travel. In order to avoid delay in operational travel, the Participating Agency will provide general travel authority to all of its participating employees for the duration of the employee's membership in the JTTFs. For domestic travel, each agency member will be responsible for appropriate notifications within his or her own agency, as well as standard FBI travel approvals and notification. The FBI will obtain FBIHQ authorization and country clearances for all JTTF members who are required to travel outside the United States. As noted above, the appropriate security clearance must be obtained prior to any international travel. The FBI will pay costs for travel of all members of the JTTFs to conduct investigations outside of the JTTF's assigned territory.

XIII. VEHICLES AND EQUIPMENT

A. In furtherance of this MOU, employees of the Participating Agency may be permitted to drive FBI owned or leased vehicles for surveillance, case management and investigation in connection with any JTTF investigation. FBI vehicles must only be used for official JTTF business and only in accordance with applicable FBI rules and regulations.

B. *[non-Federal entities only]* Any civil liability arising from the use of an FBI owned or leased vehicle by a Participating Agency task force member while engaged in any conduct other than his or her official duties and assignments under this MOU shall not be the responsibility of the FBI or the United States. To the extent permitted by applicable law, the Participating Agency will hold harmless the FBI and the United States for any claim for property damage or personal injury arising from any use of an FBI owned or leased vehicle by a Participating Agency JTTF member which is outside of the scope of his or her official duties and assignments under this MOU.

C. For official inventory purposes, all JTTF equipment including badges, credentials and other forms of JTTF identification subject to FBI property inventory requirements will be produced by each JTTF member upon request. At the completion of the member's assignment on the JTTF, or upon withdrawal or termination of the Participating Agency from the JTTF, all equipment will be returned to the supplying agency.

XIV. FORFEITURE

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

The FBI shall be responsible for the processing of assets seized for federal forfeiture in conjunction with JTTF operations, as provided by these rules and regulations. Asset forfeitures will be conducted in accordance with federal law and the rules and regulations set forth by the U.S. Department of Justice and the FBI. Forfeitures attributable to JTTF investigations may be distributed among the Participating Agencies in JTTF-related operations at the discretion of the FBI.

XV. HUMAN SOURCES

A. All human sources developed through the JTTF will be handled in accordance with the Attorney General's and the FBI's guidelines, policies and procedures.

B. All human sources developed during the course of any JTTF investigation shall be operated with all appropriate FBI suitability paperwork completed prior to use. All source debriefings or written products of information obtained from any human source will use FBI document format and handling procedures.

C. The FBI, as permitted by federal law, agrees to pay reasonable and necessary human source expenses incurred by the JTTF. All expenses must be approved by the FBI before they are incurred. No payments may be made to JTTF human sources without prior FBI approval.

XVI. MEDICAL

A. All Participating Agencies will ensure that detailed JTTF members are medically qualified according to their agencies' standards to perform law enforcement duties, functions and responsibilities.

B. To ensure protection for purposes of the Federal Employees' Compensation Act (FECA), JTTF members should be detailed to the FBI consistent with the provisions of the Intergovernmental Personnel Act (IPA), 5 U.S.C. § 3374(d). This Act stipulates that "[a] State or local government employee who is given an appointment in a Federal agency for the period of the assignment or who is on detail to a Federal agency and who suffers disability or dies as a result of personal injury sustained while in the performance of his duty during the assignment shall be treated . . . as though he were an employee as defined by section 8101 of this title who has sustained the injury in the performance of duty." Other provisions of federal law may extend FECA benefits in more limited circumstances. The Department of Labor's Office of Workers' Compensation Programs is charged with making FECA coverage determinations and is available to provide guidance concerning specific circumstances.

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

XVII. TRAINING

All JTTF members are required to attend FBI legal training in compliance with FBI regulations and any other training deemed necessary by the FBI chain of command. The FBI is responsible for the costs of such training. The Participating Agency will bear the costs of any training required of its own employees detailed to the JTTF.

XVIII. DEADLY FORCE AND SHOOTING INCIDENT POLICIES

Members of the JTTF will follow their own agency's policy concerning use of deadly force.

XIX. DEPARTMENT OF DEFENSE COMPONENTS

The Posse Comitatus Act, 18 U.S.C. § 1385, prohibits the Army and Air Force (Department of Defense regulations now restrict the activities of all branches or components of the Armed Services under this Act) from being used as a posse comitatus or otherwise to execute the laws entrusted to civilian law enforcement authorities. The restrictions of the Act do not apply to civilian employees of the Department of Defense who are not acting under the direct command and control of a military officer. Other statutory provisions specifically authorize certain indirect and direct assistance and participation by the military in specified law enforcement functions and activities. All Department of Defense components (except strictly civilian components not acting under direct command and control of a military officer) who enter into this agreement, shall comply with all Department of Defense regulations and statutory authorities (describing restrictions, authorizations and conditions in support of law enforcement) including but not limited to Department of Defense Directives 5525.5, and 3025.15, Chapter 18 of Title 10 of the United States Code dealing with military support for civilian law enforcement agencies and any other or subsequent rules, regulations, and laws that may address this topic or that may amend, or modify any of the above provisions. This MOU shall not be construed to authorize any additional or greater authority (than already described) for Department of Defense components to act in the support of law enforcement activities.

XX. MEDIA

All media releases will be mutually agreed upon and jointly handled by the member Participating Agencies of the appropriate JTTF. Press releases will conform to DOJ Guidelines regarding press releases. No press release will be issued without prior FBI approval.

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

XXI. LIABILITY

The Participating Agency acknowledges that financial and civil liability, if any and in accordance with applicable law, for the acts and omissions of each employee detailed to the JTTF remains vested with his or her employing agency. However, the Department of Justice (DOJ) may, in its discretion, determine on a case-by-case basis that an individual should be afforded legal representation, legal defense, or indemnification of a civil judgment, pursuant to federal law and DOJ policy and regulations.

A. COMMON LAW TORT CLAIMS

1. Congress has provided that the exclusive remedy for the negligent or wrongful act or omission of an employee of the U.S. Government, acting within the scope of his or her employment, shall be an action against the United States under the FTCA, 28 U.S.C. § 1346(b), and §§ 2671 - 2680.

2. Notwithstanding the provisions contained in Article XIII of this MOU, for the limited purpose of defending civil claims arising out of JTTF activity, a state, local, or tribal law enforcement officer who has been federally deputized and who is acting within the course and scope of his or her official duties and assignments pursuant to this MOU may be considered an "employee" of the U.S. government, as defined at 28 U.S.C. § 2671. See 5 U.S.C. § 3374(c)(2).

3. Under the Federal Employee Liability Reform and Tort Compensation Act of 1998 (commonly known as the Westfall Act), 28 U.S.C. § 2679(b)(1), if an employee of the United States is named as a defendant in a civil action, the Attorney General or his or her designee may certify that the defendant acted within the scope of his or her employment at the time of the incident giving rise to the suit. 28 U.S.C. § 2679(d)(2). The United States can then be substituted for the employee as the sole defendant with respect to any tort claims alleged in the action. 28 U.S.C. § 2679(d)(2). If the United States is substituted as defendant, the individual employee is thereby protected from suit on any tort claim arising out of the incident.

4. If the Attorney General declines to certify that an employee was acting within the scope of employment, "the employee may at any time before trial petition the court to find and certify that the employee was acting within the scope of his office or employment." 28 U.S.C. § 2679(d)(3).

**This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.**

5. Liability for any negligent or willful acts of JTTF members undertaken outside the terms of this MOU will be the sole responsibility of the respective employee and agency involved.

B. CONSTITUTIONAL CLAIMS

1. Liability for violations of federal constitutional law may rest with the individual federal agent or officer pursuant to Bivens v. Six Unknown Names Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) or pursuant to 42 U.S.C. § 1983 for state officers.

2. Federal, state, local, and tribal officers enjoy qualified immunity from suit for constitutional torts, "insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." Harlow v. Fitzgerald, 457 U.S. 800 (1982).

3. If a Participating Agency JTTF officer is named as a defendant in his or her individual capacity in a civil action alleging constitutional damages as a result of conduct taken within the course of the JTTF, the officer may request representation by DOJ. 28 C.F.R. §§ 50.15, 50.16.

4. An employee may be provided representation "when the actions for which representation is requested reasonably appears to have been performed within the scope of the employee's employment, and the Attorney General, or his or her designee, determines that providing representation would otherwise be in the interest of the United States." 28 C.F.R. § 50.15(a).

5. A JTTF member's written request for representation should be directed to the Attorney General and provided to the Chief Division Counsel (CDC) of the FBI division coordinating the JTTF. The CDC will forward the representation request to the FBI's Office of the General Counsel (OGC), together with a letterhead memorandum concerning the factual basis of the lawsuit. FBI's OGC will then forward the request to the Civil Division of DOJ, together with an agency recommendation concerning scope of employment and DOJ representation. 28 C.F.R. § 50.15(a)(3).

6. If a JTTF member is found to be liable for a constitutional tort, he or she may request indemnification from DOJ to satisfy an adverse judgement

This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

rendered against the employee in his or her individual capacity. 28 C.F.R. § 50.15(c)(4). The criteria for payment are substantially similar to those used to determine whether a federal employee is entitled to DOJ representation under 28 C.F.R.§ 50.15(a).

7. Determinations concerning legal representation and indemnification by the United States are discretionary and are made by DOJ on a case-by-case basis. The FBI cannot guarantee that the United States will provide legal representation, legal defense, or indemnification to any federal or state employee detailed to the JTTF, and nothing in this Article shall be deemed to create any legal right on the part of any JTTF personnel.

C. EXPRESS RESERVATIONS

1. Nothing in this Article shall be deemed to create an employment relationship between the FBI or the United States and any Participating Agency JTTF member other than for exclusive purposes of the FTCA, as outlined herein.

2. The participating agencies do not waive any available defenses and/or limitations on liability. No Participating Agency shall be considered to be an agent of any other Participating Agency.

XXII. DURATION

A. The term of the MOU shall be an indefinite period. The MOU may be terminated at will by any party, provided written notice is provided to the other parties of not less than sixty (60) days. Upon termination of the MOU, all equipment will be returned to the supplying agency(ies). It is understood that the termination of this agreement by any one of the Participating Agencies will have no effect on the agreement between the FBI and all other participating agencies.

B. Notwithstanding this provision, the provisions of Paragraph IX, entitled RECORDS, REPORTS AND INFORMATION SHARING, and Paragraph XXI. entitled LIABILITY, will continue until all potential liabilities have lapsed. Similarly, the inherent disclaimer limitation contained in the EXPRESS RESERVATION provision will survive any termination.

FOR OFFICIAL USE ONLY
This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

XXIII. AMENDMENTS

This agreement in no manner affects any existing MOUs or agreements with the FBI or any other agency. This agreement may be amended only by mutual written consent of the parties. The modifications shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of the FBI and the Participating Agency.

SIGNATORIES:

_____ Date: _____

_____ Date: _____

_____ Date: _____

Contracting Officer
Federal Bureau of Investigation
Washington, D.C.

FOR OFFICIAL USE ONLY
This document is the property of the FBI and is loaned to your agency.
Neither it nor its contents may be released without authorization by FBI Headquarters.

MASS JTTF-442

BOSTON
JOINT TERRORISM TASK FORCE
MEMORANDUM OF AGREEMENT

PREAMBLE

This Memorandum of Agreement (MOA) is entered into by the Federal Bureau of Investigation (FBI) and the Massachusetts State Police (MSP) and outlines a cooperative effort to combat terrorism.

ARTICLE ONE:

PURPOSE OF MOA

This MOA establishes and delineates the mission and structure of the Boston Joint Terrorism Task Force (JTTF) in addressing the complex problem of terrorism affecting the New England states of Massachusetts, Maine, New Hampshire, and Rhode Island.

The purpose of this MOA is to set out a common understanding of the policies and procedures the Massachusetts State Police and the FBI will follow in providing law enforcement service to the citizens of Massachusetts and the United States of America.

ARTICLE TWO:

MISSION OF THE JTTF

The mission of the JTTF will be to utilize the collective resources of the participating agencies for the prevention, preemption, deterrence and investigation of terrorism and activities related to terrorism, both actual and potential, occurring in or affecting the U.S. carried out by terrorist groups and/or individuals, as well as apprehending individuals committing such violations. All parties agree to abide by the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (AG Guidelines) and the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations as they pertain to International Terrorism matters. In addition, it is understood that personnel of the MSP shall be required to utilize only those investigative techniques consistent with their given standards and procedures.

ARTICLE THREE:

ORGANIZATIONAL STRUCTURE AND MANAGEMENT OF THE TASK FORCE

A. MEMBERS

The JTTF shall consist of personnel of the [redacted] b7E

[redacted], and the Federal Bureau of Investigation (FBI).

B. IDENTIFICATION OF OBJECTIVES

The Special Agent in Charge (SAC) of the FBI and the participating agencies of the JTTF shall identify, agree upon, and articulate specific organizations and investigative objectives or matters assigned to the JTTF.

C. DIRECTION OF JTTF AND RESOURCE CONTROL

Responsibility for the overall policy and direction of the JTTF shall rest with an Assistant Special Agent in Charge (ASAC) of the FBI, who will closely coordinate with the Colonel of the Massachusetts State Police or their designees, on matters of mutual concern relating to such policy and direction, thus ensuring the absence of conflict.

Specific control over their JTTF resources and the continued dedication of these resources to the JTTF shall be retained by the participating agency heads, who will be kept fully apprized of all investigative developments by their respective subordinates.

D. SUPERVISION OF JTTF

The direct day-to-day supervision for matters assigned to the JTTF shall be the responsibility of the designated FBI Supervisory Special Agent (SSA) in conjunction with the designated supervisory personnel of the Massachusetts State Police. The FBI SSA will be responsible for administrative/operational matters directly associated with his/her Squad and the JTTF, such as assigning cases, shifts, and completion of written work necessary to make each squad and the JTTF operative and functional. Responsibility for the conduct of the JTTF members shall remain with the respective agency heads. All JTTF personnel will keep their respective superiors completely informed of pertinent developments.

E. PHYSICAL LOCATION AND SUPPORT

The FBI will provide office space for all JTTF members and support staff. In addition, the FBI will provide all necessary secretarial, clerical, automation and technical support for the

JTTF.

F. COMMITMENT OF PERSONNEL

The FBI will assign [redacted] SSA [redacted] and [redacted] Special Agents. [redacted] will assign [redacted] Detectives and from [redacted] In addition, [redacted] investigators from [redacted] will be assigned to the FBI Hazmat Response Team. b7E

All members of the JTTF, with the exception of the [redacted] will be assigned full-time to the JTTF. Continued assignment of members will be made at the discretion of their respective agencies consistent with FBI and MSP guidelines. b7E

ARTICLE FOUR:

VEHICLES

The JTTF agrees to provide the MSP task force members with a vehicle. The purpose of these vehicles is for surveillance, case management and investigation in connection with any JTTF investigation. The vehicle provided by the FBI can be used for official use only in connection with matters investigated by the JTTF.

In furtherance of the mission of the JTTF and in compliance with existing FBI policy for operation of U.S. Government vehicles, the FBI hereby agrees and authorizes members of the MSP participating in the JTTF to operate vehicles owned or leased by the FBI.

The MSP agrees to be responsible for tortious acts or omissions on the part of the MSP or their employees, and for any liability resulting from use of FBI owned or leased vehicles utilized by the MSP Task Force members, and for any damage to said vehicles as a result of any tortious action or omission on the part of the MSP or their employees.

ARTICLE FIVE:

RECORDS AND REPORTS

All JTTF investigative records will be maintained at the [redacted] FBI. Investigative reports will be prepared on FBI forms. Decisions for placement of all or part of said investigative records into MSP files or data bases shall rest with supervisory personnel of the FBI and the MSP in compliance with applicable standards and procedures governing the respective parties. Classified information will not be placed in MSP files. b7E

ARTICLE SIX:

SECURITY CLEARANCE/DEPUTATION

Due to various United States, Department of Justice and FBI regulations and laws regarding classified information, prospective members of the JTTF who do not possess Top Secret clearances previously granted by the FBI/DOJ will be subjected to full background investigation(s) with assignment contingent upon receipt of appropriate security clearances(s). All non-FBI personnel will be sworn in as Special Deputy United States Marshals. Security clearances will be granted for any applicable and relevant MSP managers or Supervisors up to, and including, the Colonel. Investigative restrictions imposed by the MSP shall not be voided by deputation of their respective personnel. All members of the JTTF shall agree not to disclose any classified or sensitive information to non JTTF members without the express permission of the FBI and shall agree to execute any applicable non-disclosure agreements, as may be necessary or required by the FBI.

ARTICLE SEVEN:

INVESTIGATIVE EXCLUSIVITY

It is agreed that matters designated to be handled by the JTTF will not knowingly be subject to non-JTTF law enforcement efforts. Recognizing the amount of specialized entities within each member agency, it is incumbent upon each agency to make proper internal notification regarding JTTF existence, including its areas of concern. All information developed by the individual member agency, in the course of investigations prior to the JTTF, will be referred to the JTTF for review and coordination, with approval of the command staff of each member agency. The non-specialized entities of each member agency handle a myriad of different law violations; therefore, JTTF members should make an effort to keep abreast of law enforcement developments within their respective agencies, to ensure information involving JTTF members is referred to the JTTF.

It is also agreed there shall be no unilateral action taken on the part of any participating agency relating to JTTF investigations. All law enforcement actions will be coordinated and cooperatively carried out.

ARTICLE EIGHT:

SALARY/COMPENSATION

Salaries of JTTF members will be paid by their respective agencies. Overtime incurred in the performance of JTTF responsibilities, when allowable under federal law and to the extent that federal funding is available for such purposes, will be reimbursed by the FBI so long as a separate overtime agreement is executed between the parties. Otherwise, overtime shall be

compensated in accordance with applicable MSP overtime provisions and shall be subject to the prior approval of appropriate personnel.

ARTICLE NINE:

PROSECUTION

JTTF investigations will conform to the requirements of federal prosecution rules and regulations and will generally be prosecuted in federal courts. It is recognized, however, that specific circumstances may, on a case-by-case basis, indicate that prosecution should be in a state court. The criteria for making such decisions will focus upon achieving the greatest overall benefit to law enforcement and the public, and effecting the greatest impact on terrorism.

ARTICLE TEN:

INFORMANTS/EXPENSES

The JTTF will abide by the Attorney General's Guidelines on the Use of Informants and Confidential Sources. To the extent that MSP standards and procedures impose any greater restrictions upon the use of their informants and cooperating witnesses, such personnel shall be bound by those restrictions. Subject to appropriate FBI approvals, the FBI agrees to pay any reasonable and necessary expenses incurred by the JTTF. The MSP agrees that prior to incurring such expenses, it will consult with the FBI's designated representative to ensure anticipated expenses will be in furtherance of JTTF goals and objectives.

ARTICLE ELEVEN:

FORFEITURE

Any forfeiture realized as a result of cases worked by the JTTF will be handled in accordance with applicable federal law and FBI guidelines. FBI guidelines will govern the sharing of seized and/or forfeited assets.

ARTICLE TWELVE:

MEDIA

No members of the JTTF will discuss or otherwise reveal information relating to JTTF investigations, or other FBI related investigations known to them, to any media representatives. All media releases on JTTF matters will be mutually agreed upon and coordinated jointly.

ARTICLE THIRTEEN:

LIABILITY

Unless specifically addressed by the terms of this MOA, the parties agree to be responsible for the negligent or wrongful acts or omissions of their respective employees. Legal representation by the United States is determined by the Department of Justice (DOJ) on a case-by-case basis. The FBI cannot guarantee the United States will provide legal representation to any Federal or state law enforcement officer or employee.

Congress has provided that the exclusive remedy for the negligent or wrongful act or omission of an employee of the United States government, acting within the scope of his/her employment, shall be an action against the United States under the Federal Tort Claims Act (FTCA), 28 U.S.C. Section 1346(b), and Sections 2671 - 2680.

For the limited purpose of defending claims arising out of JTTF activity, state officers who have been specifically deputized and who are acting within the course and scope of their official duties and assignments pursuant to this MOA, may be considered an "employee" of the United States Government as defined in 28 U.S.C. Section 2671. See 5 U.S.C. Section 3374(c)(2).

Under the Federal Employees Liability Reform and Tort Compensation, Act of 1998 (commonly known as the Westfall Act), 28 U.S.C., Section 2679(b)(1), the Attorney General or his/her designee may certify that an individual defendant acted within the scope of his employment at the time of the incident giving rise to the suit. id., 28 U.S.C. Section 2679(d)(2). The United States can then be substituted for the employee as the sole defendant with respect to any tort claims. 28 U.S.C. Section 2679(d)(2). If the United States is substituted as defendant, the individual employee is thereby protected from suits in his official capacity.

If the Attorney General declines to certify that an employee was acting within the scope of employment, "the employee may at any time before trial petition the court to find and certify that the employee was acting within the scope of his office or employment." 28 U.S.C. Section 2679(d)(3).

Liability for any negligent or willful acts of JTTF members, undertaken outside the terms of this MOA will be the sole responsibility of the respective employee and agency involved.

Liability for violations of federal constitutional law rests with the individual federal agent or officer pursuant to Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388 (1971) or pursuant to 42 U.S.C. Section 1983 for state officers or cross-deputized federal officers.

Both state and federal officers enjoy qualified immunity from

suit for constitutional torts, "insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known." Harlow v. Fitzgerald, 457 U.S. 800 (1982).

JTTF officers may request representation by the U. S. Department of Justice for civil suits against them in their individual capacities for actions taken within the scope of employment. 28 C.F.R. Sections 50.15, 50.16.

An employee may be provided representation "when the actions for which representation is requested reasonably appear to have been performed within the scope of the employee's employment and the Attorney General, or his/her designee, determines that providing representation would otherwise be in the interest of the United States." 28 C.F.R. Section 50.15(a).

A JTTF officer's written request for representation should be directed to the Attorney General and provided to the Chief Division Counsel (CDC) of the FBI division coordinating the task force. The CDC will then forward the representation request to the FBI's office of General Counsel (OGC) together with a letterhead memorandum concerning the factual basis for the lawsuit. FBI/OGC will then forward the request to the Civil Division of DOJ together with an agency recommendation concerning scope of employment and Department representation. 28 C.F.R. Section 50.15 (a)(3).

If a JTTF officer is found to be liable for a constitutional tort, he/she may request indemnification from DOJ to satisfy an adverse judgement rendered against the employee in his/her individual capacity. 28 C.F.R. Section 50.15 (c)(4). The criteria for payment are substantially similar to those used to determine whether a federal employee is entitled to DOJ representation under 28 C.F.R. Section 50.15(a).

ARTICLE FOURTEEN:

DURATION OF THE TASK FORCE

The JTTF will continue for an indefinite period but participation may be terminated at any time upon the written notice of either party to this Memorandum of Agreement.

SIGNATORIES:

Richard DesLauriers 1/20/12

~~CHARLES S. PROUTY~~ Richard DesLauriers
SPECIAL AGENT IN CHARGE
Federal Bureau of Investigation
Boston, Massachusetts

Thomas J. Foley 1/17/03

COLONEL THOMAS FOLEY
Massachusetts State Police
Framingham, Massachusetts

Curtis Bolint 12/29/02

Office of the Chief Contracting Officer
Federal Bureau of Investigation
Washington, D.C.

REIMBURSEMENT AGREEMENT
BETWEEN THE FEDERAL BUREAU OF INVESTIGATION
AND
MASSACHUSETTS STATE POLICE

Pursuant to Fiscal Year 2003 appropriations as authorized by Congress, overtime to police officers assigned to this task force, for expenses necessary for detection, investigation, and prosecution of crimes against the United States is authorized subject to the limits set forth in the budget for this task force as approved by the Counterterrorism Division, Federal Bureau of Investigation (FBI), and subject to specific provisions and conditions as set forth in this Reimbursement Agreement. Therefore, it is hereby agreed between the FBI and the Massachusetts State Police (hereinafter referred to as "agency") that:

1. The FBI will reimburse the agency for overtime payments made to officers assigned full-time to the Boston Joint Terrorism Task Force (JTTF). The agency will have [redacted] full-time officers assigned to the JTTF and the number of agency officers entitled to reimbursement in Fiscal Year 2003 shall not exceed [redacted]. b7E

2. Requests for reimbursement shall be made on a monthly basis and should be forwarded to FBI Headquarters as soon as practicable after the first of the month which follows the month for which reimbursement is requested. Such requests should be forwarded by the appropriate agency supervisor(s) to the FBI Task Force Squad Supervisor and Special Agent-in-Charge for their review, approval and submission.

3. Overtime payments shall be made payable to and mailed directly to the agency by the FBI.

4. Overtime reimbursement will be calculated at the usual rate for which the individual officers' time would be compensated in the absence of this agreement. However, the FBI will only reimburse the agency for overtime paid to the officers who work full-time in support of the JTTF in Fiscal Year 2003 (October 1, 2002 to September 30, 2003) up to a total amount of [redacted] per officer per year. Additionally, reimbursement for any one month period shall not exceed [redacted] per officer. b7E

5. Each request for consideration shall include the name, rank, identification number, overtime compensation rate, number of reimbursable hours claimed and the dates of those hours for each officer for whom reimbursement is sought. Each reimbursement request must be accompanied by a certificate signed by an appropriate supervisor of the submitting department that

the request has been personally reviewed, that the information described in this paragraph is accurate, and the personnel for whom reimbursement is claimed were assigned full-time to JTTF cases.

6. This agreement may be modified at any time by written consent of the parties. This agreement may be terminated at any time by either party and shall not extend beyond September 30, 2003.

By: _____ Date: 12/29/02
Office of the Chief
Contracting Officer, FBI

By: _____ Date: 1/20/12
~~Charles S. Prouty~~ Richard DesLauriers
Special Agent-in-Charge
Federal Bureau of Investigation
Lowell, Massachusetts

By: _____ Date: 1/17/03
Colonel Thomas Foley
Massachusetts State Police
Framingham, Massachusetts

DECLASSIFIED BY NSICG F54M93K42
ON 10-08-2014

FD-1057 (Rev. 5-8-10)

~~SECRET~~

OFFICIAL RECORD

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) JTTF Executive Board Meeting, September 26, 2013.

Date: 10/08/2013

From: BOSTON
[redacted]
Contact: [redacted]

b6
b7C
b7E

Approved By: A/SSA [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (U) DOCUMENTATION OF EXECUTIVE BOARD MEETINGS (U)

Synopsis: (U) To document the Boston JTTF Executive Board Meeting, held September 26, 2013.

~~**Reason: 1.4(b), (c), (d)**~~
~~**Derived From: FBI**~~
~~**NSISC-20090615**~~
~~**Declassify On: 20381007**~~

Details:

The Boston JTTF sponsored the fourth FY 2013 Executive Board meeting in Boston, Massachusetts on Thursday, September 26, 2013. The meeting was attended by senior level executives from approximately 40 agencies.

The JTTF Executive Board members were presented with a classified national security briefing which included the following: (1) current international and domestic terrorism trends; (2) regional case updates on JTTF cases in Boston's area of responsibility. Representatives from the following agencies were in attendance:

AGENCY

~~SECRET~~

~~SECRET~~

Title: (U) JTTF Executive Board Meeting, September 26, 2013.
Re: [redacted], 10/08/2013 b7E

b7E

[redacted]

~~SECRET~~

~~SECRET~~

Title: (U) JTTF Executive Board Meeting, September 26, 2013.
Re: [redacted] 10/08/2013 b7E

[redacted] b7E

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-08-2014 BY NSICG F54M93K42

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/09/2007

To: Counterterrorism **Attn:** [redacted]/NJTTF b7E

From: Boston
[redacted]
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 319T-HQ-A1487667-CTD (Pending)-1520
319W1-HQ-A1487697-BS (Pending)

Title: JOINT TERRORISM TASK FORCE (JTTF) PROGRAM
STANDARD MEMORANDUM OF UNDERSTANDING FOR JTTF

Synopsis: Provide copies of Standard MOU to NJTTF.

Reference: [redacted] b7E

Enclosure(s): Enclosed for NJTTF are signed copies of Standard Memorandum of Understanding (MOU) received as of 05/09/2007.

Details: Attached to this communication are signed copies of the Standard Memorandum of Understanding (MOU) for the following law enforcement agencies:

1. City of Portland Police Dept.
2. Rhode Island State Police
3. City of Providence Police Dept.
4. Massachusetts Bay Transit Authority Police Dept.
5. City of Boston Police Dept.
6. New Hampshire State Police
7. City of Manchester Police Dept.
8. City of Lowell Police Dept.
9. City of Worcester Police Dept.
10. City of Holyoke Police Dept.
11. City of Pittsfield Police Dept.
12. City of Springfield Police Dept.
13. City of West Springfield Police Dept.
14. Massachusetts Department of Corrections

FBI Boston is awaiting signed copies from;

To: Counterterrorism From: Boston
Re: 319T-HQ-A1487667-CTD, 05/09/2007

b7E

1.
2.
3.

FBI Boston JTTF will continue to pursue the signing of these MOU's and forward to NJTTF via separate correspondence once they are received.

To: Counterterrorism From: Boston
Re: 319T-HQ-A1487667-CTD, 05/09/2007

LEAD(s):

Set Lead 1: (Info)

COUNTERTERRORISM

AT NJTTF

Copies of Standard MOU provided to NJTTF.

♦♦

mistress america
august 14

The New York Times

U.S.

F.B.I. Focusing on Security Over Ordinary Crime

By **CHARLIE SAVAGE** AUG. 23, 2011

WASHINGTON — Agents of the Federal Bureau of Investigation have been more likely to be hunting for potential threats to national security than for ordinary criminals in recent years, but much of the time found neither, according to newly disclosed internal information.

Data from a recent two-year period showed that the bureau opened 82,325 assessments of people and groups in search for signs of wrongdoing. Agents closed out most of the assessments, the lowest-level of F.B.I. investigation, without finding information that justified a more intensive inquiry.

Separately, the bureau also initiated 1,819 assessments during the period to identify any possible threats within particular geographic districts. That activity ranged from looking for the presence of particular organizations, like gangs or terrorist groups with definable characteristics, to evaluating other potential vulnerabilities, like a university with classified research and many foreign students.

The data, obtained by The New York Times under the Freedom of Information Act, offers a panoramic view of the bureau's activities toward the end of a decade-long effort to transform the F.B.I. from a law-enforcement

agency focused on solving crimes to a domestic intelligence agency whose mission is to detect potential threats before they can reach fruition.

The disclosure, covering March 25, 2009, to March 31, 2011, focused on assessments, which an agent may open "proactively or in response to investigative leads" and without first having a particular factual basis for suspecting a target of wrongdoing, according to the F.B.I. manual. Former Attorney General Michael Mukasey issued guidelines for the bureau creating that category in 2008.

During an assessment, agents may use a limited set of techniques, including searching databases about targets, conducting surveillance of their movements and sending a confidential informant to an organization's meetings. But to use more intrusive techniques, like secretly reading e-mail, agents must open a more traditional "preliminary" or "full" investigation. Such inquiries require agents to first have a greater reason to start scrutinizing someone: either an "information or allegation" or an "articulable factual basis" indicating possible wrongdoing.

According to the data, during the 2009-11 period agents opened 42,888 assessments of people or groups to see whether they were terrorists or spies. A database search in May 2011 showed that 41,056 of the assessments had been closed. Information gathered by agents during those assessments had led to 1,986 preliminary or full investigations.

The data also showed that agents initiated 39,437 assessments of people or groups to see whether they were engaged in ordinary crime. Of those, 36,044 had been closed, while 1,329 preliminary or full investigations had been opened based on the information gathered.

Michael German, a former F.B.I. agent who is now with the American Civil Liberties Union, said the high number of assessments relative to the number that developed into more intensive investigations was cause for concern. He noted that the F.B.I. retained the data it collects about a target,

even if the person or group turns out to be innocent.

"It's clear the F.B.I. is casting its investigative net too broadly," Mr. German said. "And remember that only a small proportion of 'preliminary' investigations become 'full' investigations, and only a small percentage of full investigations result in criminal charges. This data makes it clear that the 'assessment' authority granted in the attorney general guidelines is far too broad."

But Valerie E. Caproni, the F.B.I. general counsel, said that the data showed that agents had been able to dispose of about 96 percent of the low-grade reasons they might have had for suspecting someone of wrongdoing, like a vague tip or some other ambiguous lead, using "low intrusion techniques" rather than by opening a potentially more invasive preliminary investigation.

The new investigation standards, Ms. Caproni said, "end up being privacy protective because previously, without a well-developed, robust assessment category, many if not most of those would have been opened as preliminary investigations."

The newly disclosed data roughly matched a far more limited disclosure earlier this year about assessments of people and groups generated in late 2008 and early 2009, but the latest data covered a longer period and included additional detail. The data also bolsters the F.B.I.'s assertion that since the Sept. 11 attacks, the bureau has taken low-grade tips about national security threats more seriously than similarly vague and seemingly implausible leads about possible criminal activity. The 39,437 criminal assessments were based on 73,303 complaints received by the F.B.I., indicating that about half of the time, agents merely filled out a complaint form but saw nothing worth following up on.

In contrast, the disclosure did not offer a separate number of national security complaints, suggesting that some were not followed up with an assessment. The bureau says its policy calls for every national security-related

tip, no matter how dubious, to be investigated. Still, Ms. Caproni cautioned that the assessment data did not offer a complete view of the F.B.I.'s activities. For example, she said, if the Central Intelligence Agency told the bureau that an overseas source had provided a specific claim about a terrorist cell operating inside the United States, agents would immediately open a more intensive investigation rather than starting with an assessment.

She also cautioned that some details about the numbers might be fuzzy. In the past, for example, the F.B.I. has noted that one assessment may uncover information that leads to more than one preliminary investigation. At the same time, agents may occasionally have neglected, when opening a preliminary investigation, to record the fact that it developed out of an assessment.

The new data also showed that while the agency has opened fewer assessments looking for broader intelligence about possible threats and vulnerabilities within a district, a category it calls Type 3 assessments, it has been slower to close them. Of the 1,819 it had opened during the period, 1,056 were open by May.

Those figures covered Type 3 assessments generated both by national security programs — like domestic and international terrorism, weapons of mass destruction and counterintelligence — and criminal programs, like civil rights, gangs, organized crime, violent crime and white-collar crime. The F.B.I. censored the specific breakdown for each category. The data release comes as the F.B.I. is preparing to issue agents a new version of its manual, the Domestic Investigations and Operations Guide, that will relax some rules about the techniques allowed at the assessment stage. Ms. Caproni said the new rulebook is at the printer now, and a partly redacted version is likely to be released to the public at the same time it takes effect around mid-October.

A version of this article appears in print on August 24, 2011, on page A16 of the New York edition with the headline: F.B.I. Focusing on Security Over Ordinary Crime.